(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 1020010050111 A
(43)Date of publication of application: 15.06.2001

(21)Application number: 1020000047609
(22)Date of filing: 17.08.2000
(30)Priority: 17.08.1999 US 1999 376102

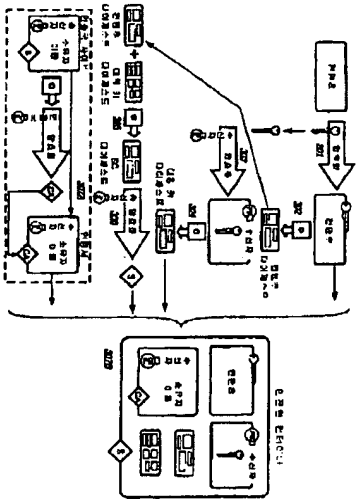
(71)Applicant: INTERNATIONAL BUSINESS MACHINES CORPORATION

(72)Inventor: DOWNS EDGAR
GRUSE GEORGE G.
HURTADO MARCO M.
LEHMAN CHRISTOPHER T.
LOTSPIECH JEFFREY B.
MILSTED KENNETH L.
SPAGNA RICHARD L.

(51)Int. Cl G06F 15/00

(54) METHOD FOR TRANSMITTING ENCRYPTION DIGITAL CONTENTS TO SYSTEM FOR PLAYING-BACK CONTENTS AND COMPUTER READABLE MEDIUM THEREFOR

(57) Abstract:



PURPOSE: A method for transmitting encryption digital contents to a system for playing-back the contents and a computer readable medium therefor are provided to securely deliver digital assets such as a printing medium, a movie, a game, and a music on the computer readable medium such as a CD and a DVD and on a global communication network such as a world wide web(WWW), and manage the right to the digital assets.

CONSTITUTION: A transmitter generates a random symmetric key and uses the generated random symmetric key for encrypting contents(301). The transmitter applies a hash algorithm to the encryption contents and generates a contents digest(302). The transmitter encrypts a symmetric key using a public key of a receiver(303). The transmitter applies the hash algorithm to the encryption symmetric key and generates a symmetric key digest(304). The transmitter applies the hash algorithm to the connection of the contents digest and the symmetric digest (305). The transmitter encrypts an SC(Security Container) using a private key of the transmitter and generates a digital signature to the SC(306). The transmitter generates an SC file including an encryption contents, an encryption symmetric key, the contents digest, and the symmetric digest, and a transmitter certificates, and an SC signature(307B). The transmitter obtains a certificates from a certificates station before starting a security communication(307A).

Legal Status
Date of final disposal of an application (20030203)
Patent registration number (1003745240000)
Date of registration (20030219)

특2001-0050111

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
G06F 15/00

(11) 공개번호 특2001-0050111
(43) 공개일자 2001년06월15일

(21) 출원번호 10-2000-0047609
(22) 출원일자 2000년08월17일
(30) 우선권주장 9/376,102 1999년08월17일 미국(US)
(71) 출원인 인터내셔널 비지네스 머신즈 코포레이션 포만 제프리 엘
미국 10504 뉴욕주 아몬크
(72) 발명자 허타도마르코엠
미국33434플로리다주보카라톤노스웨스트28번애비뉴4720
밀스테드케네스엘
미국33437플로리다주보인톤비치마제스틱웨이9927
그루스조지지
미국33064플로리다주라이트하우스포인트노스이스트24번애비뉴4310
다운스에드가
미국33308플로리다주에프티라우더데일노스이스트58번스트리트2740
레만크리스토퍼티
미국33445플로리다주딜레이비치햄프톤서클사우스2663
스파그나리차드엘
미국33498플로리다주보카라톤메플체이스드라이브10654
룻츠피치제프리비
미국95123캘리포니아주산호세푸트힐드라이브992
(74) 대리인 김창세, 김원준, 장성구

심사청구 : 있음

(54) 암호화된 디지털 컨텐츠를 컨텐츠 재생을 위한 시스템에전달하기 위한 방법 및 그를 위한 컴퓨터 판독가능 매체

요약

본원 발명은 암호화된 디지털 컨텐츠를 컨텐츠 재생을 위한 엔드 유저 시스템에 전달하는 방법에 관한 것으로, 이 방법은 이전에 컨텐츠와 연관되어 있는 메타데이터를 컴퓨터 판독가능 매체로부터 판독하는 단계를 포함하고 있다. 유저는 상기 메타데이터로부터 암호해독을 위한 연관된 컨텐츠를 선택하며, 엔드 유저 시스템은 컨텐츠를 암호해독하기 위해 인증국과 안전한 접속을 확립한다. 엔드 유저 시스템은 허가된 대로 기암호화된 컨텐츠의 적어도 일부를 암호해독하기 위한 암호해독 키를 포함하고 있는 안전한 컨테이너를 수신한다. 상기 시스템은 결제소로부터 암호화 키를 사용하여 안전한 컨테이너-여기서 이 안전한 컨테이너는 엔드드 유저 시스템으로부터의 암호화 키를 내장하고 있슴-를 생성하고, 컨텐츠를 암호해독하기 위한 허가 인증을 위해 상기 결제소로 상기 안전한 컨테이너를 전송한다. 상기 시스템은, 허가된 대로 컴퓨터 판독가능 매체 상에 저장된 기암호화된 컨텐츠의 적어도 일부를 암호해독하기 위한 상기 암호해독 키를 포함하며, 상기 엔드 유저 시스템의 상기 암호화 키를 사용하여 암호화된 안전한 컨테이너를 상기 결제소로부터 수신하며, 그리고 엔드 유저 시스템의 상기 암호화 키를 사용하여 상기 안전한 컨테이너를 암호해독하여 상기 암호화된 컨텐츠의 적어도 일부를 암호해독하는 상기 암호해독 키에 액세스함으로써 상기 기암호화된 컨텐츠의 적어도 일부를 재생한다.

대표도

도1a

명세서

도면의 간단한 설명

도 1은 본 발명에 따라 안전한 디지털 컨텐츠 전자 배포 시스템에 대한 개요를 도시한 블록도,

도 2는 본 발명에 따라 예시적 안전한 컨테이너(Secure Container:SC) 및 연관된 그래픽 표현을 도시한 블록도,

도 3은 본 발명에 따라 안전한 컨테이너에 대한 암호화 프로세스의 개요를 도시한 블록도,

도 4는 본 발명에 따라 안전한 컨테이너에 대한 암호해독 프로세스의 개요를 도시한 블록도,

도 5는 본 발명에 따라 도 1의 안전한 디지털 컨텐츠 배포 시스템의 권리 관리 구조(Rights Management Architecture)의 층들의 개요를 도시한 블록도,

도 6은 도 5의 라이센스 제어 층에 적용된 때의 컨텐츠 배포 및 라이센싱 제어의 개요를 도시한 블록도,

도 7은 본 발명에 따라 도 1의 작업 흐름 관리자 툴(Work Flow Manager Tool)에 대한 예시적 유저 인터페이스를 도시한 도면,

도 8은 본 발명에 따라 도 7의 유저 인터페이스에 대응하는 작업 흐름 관리자의 주요 툴, 구성요소 및 프로세스의 블록도,

도 9는 본 발명에 따라 도 1의 전자 디지털 컨텐츠 상점(Electronic Digital Content Store)의 주요 툴, 구성요소 및 프로세스를 도시한 블록도,

도 10은 본 발명에 따라 도 1의 엔드 유저 장치(들)(End-User Device(s))의 주요 구성요소 및 프로세스를 도시한 블록도,

도 11은 본 발명에 따라 도 8의 컨텐츠 전처리/압축 툴(Content Preprocessing and Compression tool)에 대한 인코딩 레이트 인자(encoding rate factor)를 계산하는 방법의 흐름도,

도 12는 본 발명에 따라 도 8의 자동 메타데이터 획득 툴(Automatic Metadata Acquisition Tool)에 대한 추가의 정보를 자동적으로 인출하기 위한 방법의 흐름도,

도 13은 본 발명에 따라 도 8의 전처리/압축 툴의 전처리 및 압축 파라메타를 자동적으로 세트하기 위한 방법의 흐름도,

도 14는 본 발명에 따라 도 15에 도시된 바와 같이 로컬 라이브러리로 컨텐츠를 다운로딩하는 재생기 애플리케이션(Player Application)의 유저 인터페이스 스크린의 예시도,

도 15는 본 발명에 따라 도 9의 엔드 유저 장치 상에서 동작하는 재생기 애플리케이션의 주요한 구성요소 및 프로세스를 도시한 블록도,

도 16은 본 발명에 따라 도 15의 재생기 애플리케이션의 유저 인터페이스 스크린의 예시도,

도 17은 본 발명에 따라 도 8의 자동 메타데이터 획득 툴에 대한 추가의 정보를 자동적으로 인출하는 다른 실시예에 대한 블록도,

도 18은 본 발명에 따라 컴퓨터 판독가능 저장 매체 상에 컨텐츠를 배포하기 위한 도 10의 다른 실시예에 대한 블록도,

도 19는 본 발명에 따라 디지털 컨텐츠에 대한 권리를 획득하기 위한 도 18의 그 다른 실시예의 블럭도.

도면의 주요 부분에 대한 부호의 설명

125 : 컨텐츠 처리 툴	152 : 안전한 컨테이너 패키징 툴
154 : 작업 흐름 관리자 툴	156 : 컨텐츠 판촉
160 : 데이터 베이스	

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 출원은 1999년 10월 22일에 출원된 미국 출원 번호 제09/177,096 호의 부분 계속 출원(CIP) - 이는 1998년 8월 13일에 출원된 미국 출원 번호 제 09/133,519 호의 부분 계속 출원임 - 이다. 이전 출원 번호 제09/177,096호의 전체 게시 내용은 본 명세서에 참조로 인용된다.

본 발명은 전반적으로 전자 상거래 분야에 관한 것으로, 보다 구체적으로는 CD 및 DVD 와 같은 컴퓨터 판독가능 매체 상에서 그리고 인터넷 및 월드와이드웹(WWW)과 같은 글로벌 통신 네트워크 상에서 인쇄 매체, 영화, 게임 및 음악과 같은 디지털 자산(digital assets)의 안전한 전달(secure delivery) 및 이 디지털 자산에 대한 권리 관리를 위한 시스템 및 관련 툴에 관한 것이다.

발명이 이루고자하는 기술적 과제

음악, 영화, 컴퓨터 프로그램, 화상, 게임 및 기타 컨텐츠(contents)와 같은 디지털 자산의 배포(distribution)를 위한 인터넷과 같은 글로벌 배포 시스템을 사용하는 것이 계속 증가하고 있다. 동시에, 가치있는 디지털 컨텐츠의 소유자 및 발표자(publishers)는 여러 가지 이유로 디지털 자산의 배포를 위해 인터넷을 사용하는 것에 소극적이었다. 하나의 이유는, 소유자는 디지털 컨텐츠의 검한없는 카피(copying) 혹은 표절(pirating)을 두려워한다는 것이다. 디지털 컨텐츠의 전자적 전달은 표절에 대한 여러 가지 장벽을 제거한다. 전자적 배포에 따라 제거되는 하나의 장벽은 유형의(tangible) 기록가능 매체 그 자체(예컨대, 디스켓 혹은 CD-ROM)의 필요성이다. 디지털 컨텐츠를 유형의 매체로 카피하는 데에는, 비록 많은 경우에 빈 테이프 혹은 기록가능 CD에 대한 1 달러 보다 작은 비용이더라도, 돈이 든다.

하지만, 전자적 배포의 경우, 유형의 매체가 더 이상 필요하지 않다. 유형의 매체의 비용은 컨텐츠가 전자적으로 배포되기 때문에 고려 대상이 안된다. 두 번째 장벽은 컨텐츠 자체의 포맷(format), 즉 디지털 포맷에 대한 아날로그 포맷으로 저장된 컨텐츠이다. 아날로그 포맷으로 저장된 컨텐츠, 예컨대, 인쇄된 화상과 같은 경우, 포토카피에 의해 재생되는 때, 그 카피본이 원본보다 질이 떨어진다. 종종 생성(generation)이라고 불리는 카피에 카피를 거듭할 때 마다, 원본보다 질이 떨어지게 된다. 이러한 질 저하는 화상이 디지털로 저장되는 때 더 이상 존재하지 않는다. 각각의 카피본과 카피본의 매 생성본들은 원본 만큼 선명하고 산뜻하다. 컨텐츠를 전자적으로 배포하기 위해 그리고 인터넷 상으로 넓게 컨텐츠를 배포하기 위해 매우 저렴한 비용으로 결합된 완벽한 디지털 카피의 전체 효과는 상대적으로 표절하여 권한없는 카피를 배포하는 것을 용이하게 한다. 몇 번의 키스트로크로, 표절은 인터넷 상으로 수백, 심지대 수천 개의 디지털 컨텐츠의 완벽한 카피본을 전송할 수 있다. 따라서, 전자적으로 배포되는 디지털 자산의 보호 및 보안을 확실하게 할 필요가 있다.

디지털 컨텐츠의 제공자(provider)는 컨텐츠 소유자의 권리를 보호하는 디지털 컨텐츠에 대한 안전한 글로벌 배포 시스템을 수립하기를 원한다. 디지털 컨텐츠 배포 시스템의 수립에 있어 문제는 디지털 컨텐츠의 전자 배포, 권리 관리 및 자산 보호를 위한 시스템을 개발하는 것을 포함한다. 전자적으로 배포되는 디지털 컨텐츠는 인쇄 매체, 영화, 게임, 프로그램, 텔레비전, 멀티미디어 및 음악 등의 컨텐츠를 포함한다.

전자 배포 시스템의 배치는 디지털 컨텐츠 제공자가 즉각적인 판매 통보를 통한 빠른 지불 해결과 전자적 조정을 달성할 수 있게 해줄 뿐만 아니라 컨텐츠의 재배포를 통한 2차적 수입원을 얻을 수 있게 해준다. 전자 디지털 컨텐츠 배포 시스템은 물리적인 재고품 감량(inventory outages) 혹은 반환에 의해 영향을 받지 않기 때문에, 디지털 컨텐츠 제공자 및 소매상은 비용 감소 및 이득의 개선을 실현할 수 있다. 디지털 컨텐츠 제공자는 재고품의 보다 개선된 시간 기반 판매(timed-release)를 위해, 새로운 배포 채널을 촉진하거나, 혹은 기존 배포 채널을 증대시킬 수 있다. 전자 배포 시스템으로부터의 트랜잭션 데이터(transactional data)는 전자 마케팅 프로그램 및 판촉(promotion) 상에 즉각적인 피드백을 제공하는 데 사용될 뿐만 아니라 소비자 구매 패턴에 관한 정보를 얻는 데 사용될 수 있다. 이러한 목적을 충족시키기 위해, 디지털 자산의 보호를 보장하고 디지털 자산을 계량화(metering)하는 동시에 디지털 컨텐츠 제공자가 전자 배포 모델을 사용하여 디지털 컨텐츠가 광범위한 사용자 및 비지니스에서 이용될 수 있도록 할 필요가 존재한다.

리얼 오디오, AT&T의 A2B, 리퀴드 오디오 프로 사의 리퀴드 오디오 프로(Liquid Audio Pro), 오디오 소프트의 시티 뮤직 네트워크(City Music Network), 기타 등등의 디지털 컨텐츠에 대한 다른 상업적으로 이용가능한 전자 배포 시스템들은 안정성 보장형(secured) 및 안정성 비보장형(unsecured) 전자 네트워크 상에서의 디지털 데이터의 전송을 제안한다. 안정성 보장형 전자 네트워크의 사용은 광범위한 청자로 디지털 컨텐츠를 배포하려는 디지털 컨텐츠 제공자의 요구를 상당히 감소시킨다. 웹 및 인터넷과 같은 안정성 비보장형 네트워크의 사용은 디지털 컨텐츠가 암호화의 사용을 통해 안전하게 엔드 유저(end-user)에게 도달될 수 있게 해준다. 하지만, 암호화된 디지털 컨텐츠가 일단 엔드 유저 머신 상에서 암호해독된 때, 디지털 컨텐츠는 즉시 권한없는 재배포를 위해 엔드 사용자에게 이용가능하게 된다. 따라서, 디지털 자산의 보호를 제공하고 디지털 컨텐츠가 소비자 및 비즈니스에 제공된 후에도 컨텐츠 제공자의 권리가 보장되는 안전한 디지털 컨텐츠 전자 배포 시스템에 대한 필요성이 존재한다. 따라서, 디지털 자산의 안전한 전달, 라이센싱 인증 및 사용 제어를 가능하게 하는 권리 관리에 대한 필요성이 존재한다.

디지털 컨텐츠의 소유자가 전자 배포에 소극적인 또다른 이유는, 기존의 배포 채널을 유지하고 육성하고자 하는 욕구이다. 대부분의 컨텐츠 소유자는 소매상을 통해 판매한다. 용반 시장에서, 이들 US 소매상들은 타워 레코드(Tower Records), 피치즈(Peaches), 블록버스터(Blockbuster), 서킷 시티(Circuit City) 등을 포함한다. 이들 많은 소매상들은 인터넷 사용자들이 인터넷 상에서 선택할 수 있게 하고 엔드 유저에게 선택이 메일링되게 하는 웹 싸이트를 가지고 있다. 예컨대, 용악 웹 싸이트들은 @tower, Music Boulevard 와 Columbia House를 포함한다. 전자 배포의 사용은 특히 웹 상에서, 소매점들이 자신을 다른 각각의 소매점 및 컨텐츠 소유자와 차별화할 수 있는 것을 제거할 수 있다. 따라서, 화상, 게임, 음악, 프로그램 및 비디오 따위의 전자 컨텐츠의 소매상들이 전자 배포를 통하여 음악을 판매하는 때 자신을 다른 각각의 소매상 및 컨텐츠 소유자와 차별화할 수 있는 방법을 제공할 필요가 있다.

컨텐츠 소유자는 전자 상점(electronic store)과 같은 배포 싸이트를 통한 전자 배포를 위해 디지털 컨텐츠를 마련한다. 인터넷 상의 혹은 다른 온라인 서비스를 통한 전자 상점은 자신을 그의 제품 제의(offer) 및 제품판촉에 의해 다른 상점과 차별화하기를 원한다. 전자 상점에 대응하는 비전자적 비온라인의 전통적 상점들은 제품 판촉, 제품 세일, 제품 샘플, 관대한 반환 정책 및 기타 판촉 프로그램들을 사용하여 자신을 경쟁자와 차별화한다. 하지만, 컨텐츠 제공자가 사용 조건을 디지털 컨텐츠 상에 부가하는 온라인 세계에서는, 전자 상점들이 자신을 차별화할 수 있는 능력이 극히 제한될 수 있다. 게다가, 비록 사용 조건이 변경될 수 있더라도, 전자적으로 제품을 판촉하고 판매하기 위해, 컨텐츠 제공자로부터의 디지털 컨텐츠에 연관된 메타데이터(metadata)를 처리하는 어려운 작업에 직면하게 된다. 전자 상점들은 메타데이터를 처리하는 때 여러 요건들을 관리할 필요가 있다. 첫째, 전자 상점은 컨텐츠 제공자로부터 디지털 컨텐츠와 연관된 메타데이터를 수신할 필요가 있다. 여러 번, 이 메타 데이터의 일부분들이 암호화되어 전송될 수도 있기 때문에, 컨텐츠 제공자는 암호화된 컨텐츠를 암호해독하기 위한 메카니즘을 생성하여야 한다. 둘째, 전자 상점은 제품 마케팅, 제품 위치설정 및 기타 컨텐츠에 대한 판촉 연구를 지원하기 위해, 컨텐츠가 컨텐츠 제공자로부터 수신되기 전에 혹은 컨텐츠가 전자 상점에 의해 수신된 후에, 컨텐츠 제공자로부터 메타데이터를 사전검토하기를 바란다. 셋째, 전자 상점은 그래픽 및 아티스트(artist) 정보 등의 판촉 재료에 사용되는 특정 메타데이터를 추출할 필요가 있다. 넷째, 전자 상점은 디지털 컨텐츠의 상이한 제의를 생성하기 위해 허가된 사용 조건의 일부를 수정하는 것에 의해 자신을 다른 상점과 차별하기를 원한다. 다섯째, 전자 상점은 지불 결제(payment clearance)를 위해 전자 상점를 배회할 필요 없이, 구매자에 의해 자동적으로 지불 조정(payment reconciliation)을 계정 조정소(an account reconciliation house)로 향하게 하기 위해, 메타데이터 내에서 URL과 같은 특정 어드레스를 삽입하거나 변경해야 한다. 여섯째, 전자 상점은 사용 조건과 매칭하는 저작권화된 디지털 컨텐츠의 허가된 사용을 위한 라이센스를 생성할 필요가 있을 수 있다. 예컨대, 라이센스는 디지털 컨텐츠를 한정된 수만

를 카피할 수 있는 허가권을 부여할 수 있다. 라이센스는 부여된 허가의 기간 및 조건을 반영하는 데 필요하다.

모든 이들 요건의 관점에서, 디지털 컨텐츠와 관련된 메타데이터를 처리하기 위해, 많은 전자 상점은 이들 요건을 다루기 위한 커스텀화된 소프트웨어 프로그램을 작성한다. 이들 커스텀화된 소프트웨어 프로그램을 작성하는 데 필요한 시간, 비용 및 테스팅은 클 수 있다. 따라서, 이들 요건에 대한 해결책을 제공할 필요가 있다.

더욱이, 디지털 컨텐츠의 소유자가 전자 배포에 소극적인 또다른 이유는, 전자 거래를 위한 컨텐츠를 마련하는 데에 있어 어려움이 있다는 것이다. 오늘날, 많은 컨텐츠 제공자들은 그들의 포트폴리오 내에 수백 혹은 십지어 수천 개의 타이틀을 보유한다. 음악 예에서, 컨텐츠 소유자가 단일의 마스터 사운드 레코딩(master sound recording)을 동시에 여러 상이한 포맷(예컨대, CD, 테이프 및 미니디스크) 상에 이용가능하게 하는 것은 특별한 것은 아니다. 게다가, 단일 포맷은 특정 배포 채널을 위해 마스터 사운드 레코딩이 리마스터링(re-master) 혹은 리믹싱(re-mix)되게 할 수 있다. 예로서, 브로트캐스트 라디오의 믹싱은 댄스 클럽 사운드 트랙에 대한 믹싱과는 상이할 수 있고, 또한 일반적으로 이용가능한 소비자 CD와도 상이할 수 있다. 이들 상이한 믹스(mix)에 대한 목록을 만들고 추적하는 것은 힘들 수 있다. 게다가, 마스터 레코딩의 많은 소유자들은 종종 여러번 구 레코딩(old recordings)을 여러 후속 콜렉션(collection)으로, 이를 테면 "베스트 앨범"으로,혹은 영화 음악 사운드 트랙에 대한 편집물(compilation)로 그리고 기타 콜렉션 혹은 편집물로 재발행한다. 많은 경우 제공자들은 정확한 마스터 사운드 레코딩을 선택하고 이들 사운드 레코딩이 전자 배포용 발매를 위해 전처리되고 인코딩되도록 하는 데 구 레코딩 포맷을 가이드로서 사용한다. 이는 전자 배포를 위해 구 사운 레코딩을 재발매하는 것을 지원하는 데 구 포맷을 사용하기를 원하는 컨텐츠 제공자들에 대해서 특히 그러할 수 있다. 제공자들은 인코딩 파라메타를 세트하기 위한 타이틀, 아티스트 및 사운드 레코딩을 매칭해 내기 위해 데이터베이스를 탐색할 것이다. 레코딩 포트폴리오를 위해 데이터베이스를 수동으로 탐색하는 이러한 프로세스는 단점이 없지 않다. 하나의 단점은 운영자가 수동으로 데이터베이스를 탐색하게 하고 적절하게 처리 파라메타를 세트하게 할 필요가 있다는 것이다. 따라서, 컨텐츠 제공자가 오디오 따위의 컨텐츠에 대한 연관된 데이터 및 마스터 레코딩을 자동적으로 검색할 수 있도록 하는 방법을 제공할 필요가 있다.

컨텐츠 소유자는 인코딩으로 알려진 프로세스를 통해 전자 배포를 위한 디지털 컨텐츠를 마련한다. 인코딩은 컨텐츠를 취득하고 이것이 아날로그 포맷으로 되어 있는 경우 이를 디지털화하고, 이를 압축하는 것을 수반한다. 압축 프로세스는 보다 효율적으로 디지털 컨텐츠가 네트워크 상으로 전송되고 기록가능 매체 상에 저장될 수 있게 해준다. 이는 전송 혹은 저장될 데이터의 양이 줄어들기 때문이다. 하지만, 압축은 단점이 없지 않다. 대부분의 압축은 사용될 압축 알고리즘 및 필요한 압축 레벨에 대한 결정을 필요로 한다. 예컨대, 음악의 경우, 디지털 컨텐츠, 즉 노래는 음악의 장르에 따라 매우 상이한 특성을 가질 수 있다. 한 장르에 대해 선택된 압축 알고리즘 및 압축 레벨가 또다른 장르의 음악에 대한 최적의 선택이 아닐 수 있다. 컨텐츠 제공자들은 특정의 압축 알고리즘 및 압축 레벨이 소위 롤래식과 같은 한 음악 장르에 대해 잘 동작하지만, 헤비 메탈과 같은 또다른 음악 장르에 대해서는 불만족스러운 결과를 제공함을 발견할 수 있다. 게다가, 오디오 엔지니어들은 종종 인코딩된 음악의 장르가 원하는 결과를 생성하도록 보장하기 위해, 음악을 등화(equalize)하고, 동적 범위 조정을 수행하며 다른 전처리 및 처리 세팅을 수행해야 한다. 항상 수동으로 이들 인코딩 파라메타들, 이를테면 각각의 디지털 컨텐츠에 대한 등화 레벨의 세팅 및 동적 범위 세팅 따위를 세트해야만 하는 것은 힘든 일이다. 음악 예로 돌아와서, 다양한 음악 장르를 포괄하는 콜렉션을 갖는 음악에 대한 컨텐츠 제공자는 인코딩될 각각의 노래 혹은 노래 세트에 대해 인코딩 파라메타들의 원하는 조합을 선택해야만 할 것이다. 따라서, 인코딩을 위한 처리 파라메타를 수동으로 선택해야 하는 것을 극복할 필요가 있다.

컨텐츠 압축 프로세스는 대량의 전용 계산 자원(dedicated computational resource)을 요구할 수 있다. 특히, 무삭제 장편 영화(full-length feature movies)와 같은 대형 컨텐츠 아이템에 대해서 특히 그러하다. 압축 알고리즘의 제공자는 그 압축과 연관된 다수의 트레이드오프(trade-off) 및 이점을 제시한다. 이들 트레이드오프는 컨텐츠를 압축하는 데 필요한 시간 및 계산 자원의 양, 원 컨텐츠로부터 획득된 압축량, 재생을 위한 원하는 비트 레이트, 압축된 컨텐츠의 상연 품질, 기타 인자들을 포함한다. 멀티미디어 파일을 입력 받아서 중도에 진행 정도 혹은 상태를 표시함이 없이 인코딩된 출력 파일을 생성하는 인코딩 프로그램을 사용하는 것이 문제이다. 게다가, 많은 경우, 중간 진행 상황을 표시하지 않고서 인코딩 프로그램을 호출하고 관리하는 데 다른 프로그램이 사용된다. 이로 인해, 호출하는 애플리케이션은 인코딩되도록 지정된 전체의 퍼센트 비율로서 인코딩된 컨텐츠의 양을 계측할 어떠한 방법도 갖지 못하게 된다. 호출하는 프로그램이 여러 상이한 프로그램이 동시에 실행되도록 스케쥴링하는 경우, 이는 문제가 될 수 있다. 더욱이, 이는 컨텐츠의 뱃치(batch)가 인코딩을 위해 선택되었고 컨텐츠 제공자가 인코딩 프로세스의 진행을 결정하기를 원하는 경우에 특히 문제가 될 수 있다. 따라서, 이들 문제를 해결할 필요가 있다.

디지털 컨텐츠 제공자가 그의 컨텐츠의 전자 배포에 소극적인 또다른 이유는, 전자적으로 전달된 컨텐츠를 위해 엔드 유저 장치 상에서 디지털 재생기를 생성하기 위한 표준이 없다는 것이다. 컨텐츠 제공자, 전자 상점, 혹은 전자 배포망 내의 다른 사람들은 PCS, 셋톱 박스, 포켓용 장치 등등의 다양한 장치 상에서 커스텀화된 재생기를 제공하기를 원할 수 있다. 위조(tamper)에 강한 환경, 즉 다시 말해 재생 중 제3 자에 의한 컨텐츠에 대한 권한없는 액세스를 차단하는 환경에서 디지털 컨텐츠의 암호해독을 처리할 수 있는 툴의 세트가 필요하다. 게다가, 엔드 유저가 구매한 것 이외의 컨텐츠를 사용 목적으로 액세스할 수 없게 하면서 디지털 컨텐츠의 로컬 라이브러리의 관리를 엔드 유저가 할 수 있도록 해주는 툴 세트가 필요하다.

또한, 디지털 컨텐츠 전자 배포 시스템의 또다른 문제점은 표준 전화 및 케이블 라인을 통해 컨텐츠를 다운로드하는 데 걸리는 시간의 길이다. 통신 라인 상에서 다운로드되도록 압축된 음악이 표준 전화 라인을 통해 다운로드되는 데에는 15 분 이상 걸리는 것은 흔하다. 비디오를 다운로딩하는데 필요한 시간량은 더 크다. 케이블 인터넷 액세스 및 광대역과 같은 다른 보다 높은 대역폭의 전달 시스템들이 증가하고 있음에도 불구하고, 이들 시스템은 여전히 많은 지역 및 도시에서 광범위하게 이용가능한 것은 아니다. 게다가, 많은 보다 높은 대역폭의 전달 시스템들은 접속 시간 때문에 디지털 컨텐츠 제공자와 그의

구매자 모두에게 높은 비용을 부과할 수 있다. 따라서, 큰 대역폭의 통신 접속을 필요로 함이 없이 전자 배포의 많은 이점들을 갖는 안전한 방식으로 컨텐츠를 전달하는 방법 및 장치에 대한 필요성이 존재한다. 통신 라인 상에서 그리고 컴퓨터 판독가능 매체 상에서 디지털 컨텐츠의 배포를 위한 해결책을 제공하는 것은 두 개의 이종(disparate) 시스템의 전개를 초래할 수 있다. (1) 디지털 컨텐츠 독점자의 소유권을 보호하기 위한 권리 관리, (2) 즉각적이고 정확한 보상을 위한 트랜잭션 계량화(transaction metering) 및 개방형 구조(an open architecture)에 대한 툴 및 구성요소(component)를 복제할 필요가 없이, 통신 라인 혹은 컴퓨터 판독가능 매체 중 어느 하나를 경유해 디지털 컨텐츠의 배포를 제공하는 시스템에 대한 필요가 존재한다.

디지털 컨텐츠를 보호하는 배경 상의 추가의 정보는 다음의 3가지 소스로부터 찾을 수 있다. 즉, AT&T 연구소의 잭 레시(Jack Lacy), 제임스 스니더(James Snyder), 데이빗 마허(David Maher)에 의한 "Music on the Internet and the Intellectual Property Protection Problem"(온라인 상으로 URL http://www.a2music.com/about/papers/musicipp.htm에서 이용가능함). 인터트러스트 테크놀로지사(InterTrust Technologies Corp.)의 올린 시버트(Olin Sibert), 데이빗 번스타인(David Burnstein) 및 데이빗 반 Hl(David Van Wie)의 "Cryptographically protected container, called DigiBox, in the article securing the Content, Not the Wire for Information Commerce"(URL http://www.intertrust.com/architecture/stc.html), 그리고 IBM 백서인 "Cryptolope Container Technology"(URL http://cryptolope.ibm.com/white.html)

발명의 구성 및 작용

본 발명에 따르면, 암호화된 디지털 컨텐츠를 그 재생을 위해 엔드 유저 시스템으로 전달하는 방법은, 이전에 상기 컨텐츠와 연관되어 있는 메타데이터를 컴퓨터 판독가능 매체로부터 판독하는 단계와, 상기 메타데이터로부터 암호해독할 연관된 컨텐츠를 선택하는 단계와, 상기 컨텐츠를 암호해독하기 위해 인증국(an authorization authority)과 안전한 접속(a secure connection)을 확립하는 단계와, 허가된 대로 기암호화된(previously encrypted) 컨텐츠의 적어도 일부를 암호해독하기 위해 암호해독 키를 포함하는 안전한 컨테이너(a secure container)를 수신하는 단계와, 결제소(a clearing house)로부터의 암호화 키를 사용하여 안전한 컨테이너를 생성하는 단계 -여기서, 상기 안전한 컨테이너는 상기 엔드 유저 시스템으로부터의 암호화 키를 내장하고 있음 - 상기 컨텐츠를 암호해독하는 허가의 인증을 위해 상기 결제소로 상기 안전한 컨테이너를 전송하는 단계와, 상기 결제소로부터, 허가된 대로 상기 컴퓨터 판독가능 매체 상에 저장된 기암호화된 컨텐츠의 적어도 일부를 암호해독하기 위한 상기 암호해독 키를 포함하는, 상기 엔드 유저 시스템의 상기 암호화 키를 사용하여 암호화된 안전한 컨테이너를 수신하는 단계와, 상기 암호화된 컨텐츠의 적어도 일부를 암호해독하는 상기 암호해독 키를 액세스하기 위해 상기 엔드 유저 시스템의 상기 암호화 키를 사용하여 상기 안전한 컨테이너를 암호해독하는 것에 의해, 상기 기암호화된 컨텐츠의 적어도 일부를 재생하는 단계를 포함한다.

독자가 본 실시예 내에서 빠르게 상이한 단락을 찾을 수 있도록 돕기 위해 본 발명에 대한 내용 목차가 제공된다.

13. 최종 품질 보증 프로세스(Final Quality Assurance Process)
14. 컨텐츠 배포 프로세스
15. 작업 흐름 규칙

C. 메타데이터 동화 및 진입 툴(Metadata Assimilation and Entry Tool)
1. 자동 메타데이터 획득 툴
2. 수동 메타데이터 진입 툴
3. 사용 조건 툴
4. 메타데이터 SC의 일부
5. 감독된 배포 툴

D. 컨텐츠 처리 툴
1. 워터마킹 툴
2. 전처리 및 압축 툴
3. 컨텐츠 품질 제어 툴
4. 암호화 툴

E. 컨텐츠 SC 생성 툴
F. 최종 품질 보증 툴
G. 컨텐츠 배포 툴
H. 컨텐츠 판촉 웹 싸이트(Content Promotion Web Site)
I. 컨텐츠 호스팅(Content Hosting)
1. 컨텐츠 호스팅 싸이트
2. 안전한 디지털 컨텐츠 전자 배포 시스템에 의해 제공되는 컨텐츠 호스팅 싸이트(들)(111)

IX. 전자 디지털 컨텐츠 상점
A. 개요 - 복수의 전자 디지털 컨텐츠 상점의 지원
B. 포인트-투-포인트(Point-to-Point) 전자 디지털 컨텐츠 배포 서비스
1. 통합 요건(Integration Requirements)
2. 컨텐츠 획득 툴
3. 트랜잭션 처리 모듈
4. 통지 인터페이스 모듈
5. 계정 조정 툴(Account Reconciliation Tool)
C. 브로드캐스트 전자 디지털 컨텐츠 배포 서비스

X. 엔드 유지 장치(들)
A. 개요
1. 전송 인프라 상에서의 전달
2. 컴퓨터 판독 가능 매체 상에서의 전달
B. 애플리케이션 설치
C. 안전한 컨테이너(SC) 처리기
D. 재생기 애플리케이션
1. 개요
2. 엔드 유저 인터페이스 구성요소
3. 카피/재생 관리 구성요소
4. 암호해독(1505), 압축해제(1506) 및 재생 구성요소
5. 데이터 관리(1502) 및 라이브러리 액세스 구성요소
6. 애플리케이션 간 통신 구성요소
7. 기타 구성요소

8. 포괄적 재생기(Generic Player)

Ⅰ. 안전한 디지털 컨텐츠 전자 배포 시스템(Digital Content Electronic Distribution System)

A. 시스템 개괄

안전한 디지털 컨텐츠 전자 배포 시스템(Secure Digital Content Electronic Distribution System)은, 디지털 컨텐츠 및 디지털 컨텐츠와 관련된 내용을 최종 사용자인 클라이언트 디바이스에 안전하게 배송(delivery)하고 권리를 관리하는 데 필요한 기술, 명세(specifications), 툴(tools), 소프트웨어를 망라하는 기술적 플랫폼이다. 엔드 유저 장치(들)(End-User Devices)에는 PC, 셋탑박스(IRD), 인터넷 기기(Internet appliances)들이 포함된다. 이들 장치들은 컨텐츠 소유자(content proprietors)에 의해 허가되는 바에 따라, 컨텐츠를 외부 매체 혹은 휴대용 사용자 장치에 복사할 수 있다. 디지털 컨텐츠(Digital Content) 혹은 그냥 컨텐츠(Content)라고 하는 용어는, 그림, 영화, 비디오, 음악, 프로그램, 멀티미디어, 게임을 포함하는, 디지털 포맷으로 저장된 정보와 데이터를 일컫는다.

이 기술적 플랫폼은 어떤 식으로 디지털 컨텐츠가 준비되고, 엔드 유저 장치(들)에 라이센스된 점대점(point-to-point)와 브로드캐스트 인프라(infrastructures)(가령, 케이블, 인터넷, 위성, 무선)를 통해 안전하게 분배되고, 인증되지 않은 복제 혹은 재생으로부터 보호될 지를 명시한다. 또한, 기술적 플랫폼의 구조(architecture)는 워터마킹(watermarking), 압축/인코딩, 암호화, 기타 보안 알고리즘 등이 진화함에 따라, 이들이 통합되고 발전되도록 한다.

안전한 디지털 컨텐츠 전자 배포 시스템의 기본 구성요소는, (1) 컨텐츠 소유자의 소유권을 보호하기 위한 권리 관리, (2) 적절하고 정확한 보상을 위한 트랜잭션 계량화(transaction metering), (3) 컨텐츠 제공자로 하여금, 컨텐츠를 준비하고 이것을 임의의 표준 재생기 상에서의 재생을 위해 복수의 네트워크 인프라 상으로 안전한 배송을 허락하게끔 하는 개방된, 잘 문서화된 구조이다.

1. 권리 관리

안전한 디지털 컨텐츠 전자 배포 시스템에서의 권리 관리는 시스템의 오퍼레이팅 구성요소들 간에 분산된 일련의 기능(a set of functions)들을 통하여 구현된다. 그 기본적인 기능들에는, 컨텐츠가, 안전한 라이센스를 갖는 인증된 중간 혹은 엔드 유저만이 풀 수 있도록 인증 및 제어를 라이센싱하는 것과, 복제본의 허용 회수, 재생 회수, 라이센스가 유효할 수 있는 시간적 간격 혹은 기간 등과 같은 구매 혹은 라이센스의 조건에 따라 컨텐츠의 사용을 강제하고 제어하는 것이 포함된다.

라이센싱 인증 및 제어는 결제소(들)(Clearinghouse) 개체 및 안전한 컨테이너(Secure Contairer(SC)) 기법의 사용을 통해 구현된다. 결제소(들)는 중간 혹은 엔드 유저(들)이 라이센싱 트랜잭션의 성공적인 완료의 확인 이후 컨텐츠를 풀도록 함으로써 라이센싱 인증을 제공한다. 안전한 컨테이너들은 암호화된 컨텐트 및 정보를 시스템 구성요소들 간에 배포하는 데 사용된다. SC는 인증되지 않은 간섭 혹은 전자적 정보 및 컨텐츠의 변경에 대해 보호를 제공하는 암호화, 디지털 서명, 디지털 인증을 사용하는 정보 혹은 컨텐츠의 암호화 운반체이다. 이것에 의해, 또한 디지털 컨텐츠의 인증성(authenticity) 및 진정성(integrity)의 확인이 가능하게 된다. 이들 권리 관리 기능의 잇점은, 전자 디지털 컨텐츠 분배 인프라가 안전하거나 신뢰받아야 할 필요가 없어서, 웹 및 인터넷과 같은 네트워크 인프라를 통해 전송이 가능하다는 것이다. 이는, 안전한 컨테이너 내에서 컨텐츠가 암호화되고, 그 저장 및 배포는 그것을 풀고 사용하는 것의 제어와는 별개이다라는 사실 때문이다. 암호해독 키를 가지고 있는 사용자만이 암호화된 컨텐츠를 풀 수 있으며, 결제소(들)는 인증된 적절한 사용 요구에 대해서만 암호해독 키를 발급한다. 결제소(들)는, 컨텐츠 소유자에 의해 설정된 사용 조건에 부합하지 않는 미지의 혹은 인증되지 않은 당사자 혹은 요구로부터의 가짜 요구에 대해서는 결제하지 않을 것이다. 또한, 만일 SC가 그것의 전송 동안 부당 변경(tampered)되었다면, 결제소(들) 내의 소프트웨어가 SC 내의 컨텐츠가 오손(corrupt)되었거나 혹은 위조되었다고 판단하고, 그 트랜잭션을 거부한다.

컨텐츠 사용의 제어는 엔드 유저 장치(들) 상에서 동작하는 엔드 유저 재생기 애플리케이션(End-User Player Application)(195)을 통해 가능하게 된다. 이 애플리케이션은 컨텐츠의 매 복사본(copy)마다, 2차 복제 및 재생의 허용 가능한 회수를 규정하는 디지털 코드를 내장시킨다. 디지털 코드를 생성하고, 이것을 다른 엔드 유저 재생기 애플리케이션(195)으로부터 은폐시키고, 변형 시도에 대해 대항할 수 있도록 하기 위해 디지털 워터마킹 기술이 사용된다. 다른 실시예에서, 디지털 코드는 단지 컨텐츠(113)에 연관된 사용 조건의 일부로서 보존된다. 디지털 컨텐츠(113)가 호환의(compliant) 엔드 유저 장치(들) 내에서 액세스될 때, 엔드 유저 재생기 애플리케이션(195)은 워터마크를 판독하여, 사용 제한(user restrictions)을체크하고 필요에 따라 워터마크를 갱신한다. 만일 복사본의 수가 소진되었다는 등, 컨텐츠의 요구된 사용이 사용 조건에 부합하지 않으면, 엔드 유저 장치(들)는 요구를 수행하지 않을 것이다.

디지털 워터마킹은 컨텐츠의 인증되었거나 인증되지 않은 복제본의 출처를 식별의 수단을 제공하기도 한다. 컨텐츠 소유자를 식별하고, 저작권 정보를 명시하고, 지리적인 배포 지역을 규정하고, 기타 관련 정보를 추가하기 위해 컨텐츠 소유자에 의해 컨텐츠 내에 최초 워터마크(initial watermark)가 내장된다. 컨텐츠 구매자(혹은 라이센스 수혜자(licensee)) 및 엔드 유저 장치(들)를 식별하고, 구매 혹은 라이센스 조건 및 일자를 명시하고, 기타 관련 정보를 추가하기 위해 제 2 워터마크가 컨텐츠 내에 내장된다.

워터마크는 컨텐츠의 일체적인 부분이 되기 때문에, 이들은 복사본이 인증되었는지의 여부에 관계 없이 복사본 내에 내재된다. 따라서, 디지털 컨텐츠는 컨텐츠가 어디에 상주하고 어디에서 연유하는지와는 무관하게 항상 그 소스 및 그것의 허가된 사용에 관련된 정보를 포함하고 있다. 이 정보는 컨텐츠의 불법적인 사용과 다루는 데 사용될 수 있다.

2. 계량화(Metering)

권리 관리 기능의 일부로서, 결제소(들)(Clearinghouse)는 키 교환이 결제소(들)를 통해 결제된 모든 트랜잭션의 레코드를 보관한다. 이 레코드에 의해, 라이센싱 인증 및 사용의 최초 조건(original condition)을 계량화할 수 있다. 트랜잭션 레코드는 트랜잭션 지불 및 기타의 사용의 전자적인

화해(electronic reconciliation)가 가능하도록 하기 위해 컨텐츠 소유자 혹은 컨텐츠 제공자, 소매자, 및 기타의 책임 있는 당사자에게 즉시 혹은 주기적으로 보고될 수 있다.

3. 개방형 구조

안전한 디지털 컨텐츠 전자 배포 시스템은 컨텐츠 소유자를 위한 권리 보호를 유지하면서도 시스템이 시장에서 광범위하게 설치되고 받아들여질 수 있도록, 공개된 명세 및 인터페이스를 갖는 개방형 구조이다. 시스템 구조의 융통성 및 공개성으로 인해, 시스템은 다양한 기법, 전송 인프라, 장치가 시장으로 도입됨에 따라 시간이 지남에 따라 진화할 수 있도록 되어 있다.

이 구조는 컨텐츠의 속성 및 그 포맷에 관련하여 개방되어 있다. 오디오, 프로그램, 멀티미디어, 비디오 혹은 다른 유형의 컨텐츠의 배포가 이 구조에 의해 지원된다. 컨텐츠는 디지털 음악용 선형 PCM과 같은 원시 포맷이거나, 혹은, 필터링, 압축, 혹은 프리엠퍼시스/디엠퍼시스 그 밖의 추가적인 전처리 혹은 인코딩에 의해 성취된 포맷일 수 있다. 이 구조는 여러가지 암호화 및 워터마킹 기법에 개방되어 있다. 상이한 컨텐츠 유형 및 포맷을 수용하기 위해, 그리고 이들이 진화함에 따라 새로운 기법을 도입하고 채용할 수 있도록, 특정의 기법을 선택하는 것도 가능하다. 이러한 융통성으로 인해, 컨텐츠 제공자는 안전한 디지털 컨텐츠 전자 배포 시스템 내에서 데이터 압축, 암호화, 및 포맷팅을 위해 사용하는 기법들을 선택하고 발전시킬 수 있다.

이 구조는 또한 상이한 분산 네트워크 및 분산 모델에도 개방되어 있다. 이 구조는 저속 인터넷 접속이나 고속 위성 및 케이블 네트워크에 걸쳐 컨텐츠 분배를 지원하며, 점대점 혹은 브로드캐스트 모델과도 사용할 수 있다. 또한, 이 구조는 엔드 유저 장치(들) 내의 기능들이 저가 사용자 장치를 포함하는 매우 다양한 장치 상에서 구현될 수 있도록 설계된다. 이러한 융통성으로 인해, 컨텐츠 제공자 및 소매자는 컨텐츠를 다양한 서비스 제공 기저를 통해 중간 혹은 엔드 유저에게 제공할 수 있으며, 사용자는 컨텐츠를 구입 혹은 라이센스하고, 재생하고, 다양한 호환 재생 장치 상에 이것을 기록할 수 있다.

B. 시스템 기능 요소

도 1을 참조하면, 본 발명의 안전한 디지털 컨텐츠 전자 배포 시스템(Secure Digital Content Electronic Distribution System)(100)의 개괄이 도시되어 있다. 안전한 디지털 컨텐츠 전자 배포 시스템은 컨텐츠 제공자(들)(101) 혹은 디지털 컨텐츠의 소유자, 전자 디지털 컨텐츠 상점(들)(103), 중간 시장 파트너(Intermediate Market Partner)(도시되지 않음), 결제소(105), 컨텐츠 호스팅 사이트(111), 전송 인프라(107), 엔드 유저 장치(들)(109)를 포함하는 전체적인 솔루션으로 이루어진다. 이들 각각의 시업상 요소는 안전한 디지털 컨텐츠 전자 배포 시스템(100)의 여러가지 구성요소를 사용한다. 특별히 전자 컨텐츠(113) 분포에 관련되는 사항에 대하여, 이들 사업상 요소 및 시스템 구성요소의 고수준 기술 내용에 관하여 이하 설명한다.

1. 컨텐츠 제공자(101)

컨텐츠 제공자(101) 혹은 컨텐츠 소유자는 원본 컨텐츠(113) 소유자 및/또는, 추가적인 배급을 위해 독립적인 컨텐츠(113)를 패키지하도록 인증된 배급자이다. 커텐트 제공자(101)는 자신의 권리를 직접 이용하거나, 전자 상거래의 수익과 연관된 컨텐츠 사용료 지불에 대한 댓가로, 컨텐츠(113)를 전자 디지털 컨텐츠 상점(들)(103) 혹은 중간 시장 파트너(도시되지 않음)에 라이센스할 수 있다. 컨텐츠 제공자(들)(101)의 예로서, 소니(Sony), 타임워너(Time-Warner), 엠티브이(MTV), 아이비엠(IBM), 마이크로소프트(Microsoft), 터너(Turner), 폭스(Fox) 등이 있다.

배급을 위해 컨텐츠 제공자(들)(101)는 그들의 컨텐츠(113) 및 관련 데이터를 준비하기 위해, 안전한 디지털 컨텐츠 전자 배포 시스템(100)의 일부로서 제공된 툴을 사용한다. 작업 흐름 관리자 툴(Work Flow Manager Tool)(154)은 처리될 컨텐츠(113)를 스케쥴링하고, 높은 수준의 보장이 유지되도록 하기 위해 컨텐츠(113)가 여러가지 컨텐츠(113) 준비 및 패키징 단계를 통해 흐를 때 이를 추적한다. 본 명세서 전반에 걸쳐, 컨텐츠(113)와 연관된 데이터를 의미하는 데 메타데이터라는 용어가 사용되며, 본 실시예에서는 컨텐츠(113) 자체를 포함하지는 않는다. 예를 들어, 노래에 대한 메타데이터는 노래의 제목 혹은 노래의 출처정보(credit)를 의미할 수 있지만, 노래의 사운드 레코딩(sound recording)을 의미하지는 않는다. 컨텐츠(113)는 사운드 레코딩을 포함한다. 메타데이터 동화 및 입력 툴(161)은 컨텐츠 제공자(들)의 데이터베이스(160) 혹은 컨텐츠 제공자(들)에 의해 제공된 미리 규정된 포맷의 데이터(음악의 경우의 예를 들면, CD 타이틀, 연주가 이름, 노래 곡명, CD 아트워크, 등등 컨텐츠(1130 정보)로부터 메타데이터를 추출하고, 이것을 전자 배급을 위해 패키징하는 데 사용된다. 메타데이터 동화 및 입력 툴(161)은 또한 컨텐츠(113)에 대한 사용 조건을 입력(enter)하는 데도 사용된다. 사용 조건 내의 데이터는 복제 제한 규칙, 도매 가격, 또한 필요하다고 생각되는 임의의 사업상 규칙들을 포함할 수 있다. 컨텐츠 소유자, 처리 날짜, 그리고 기타 관련 있는 데이터를 나타내는 데이터를 컨텐츠(113)에 은폐하는 데 워터마킹 툴이 사용된다. 컨텐츠(113)가 오디오인 실시예에 있어서, 최적 압축의 질로 컨텐츠(113) 혹은 다른 오디오의 동적 특성을 조절하고/하거나 등화하고, 컨텐츠(113)를 원하는 압축 레벨로 압축하고, 컨텐츠(113)를 암호화하는 데 오디오 전처리 툴이 사용된다. 이들은 디지털 컨텐츠 압축/인코딩, 암호화, 그리고 포맷팅 방법에 있어서의 기술적인 진보를 따르도록 조절될 수 있으며, 이에 따라 컨텐츠 제공자(들)(101)가 시장에서 시간에 따라 진화할 때 최상의 툴을 활용할 수 있게 된다.

암호화된 컨텐츠(113), 디지털 컨텐츠와 관련된 데이터 혹은 메타데이터, 암호화된 키가 SC 패커 툴(SC Packer Tool)에 의해 SC 내에 패킹되어, 컨텐츠 호스팅 사이트 및/또는 전자적 분배를 위한 판촉 웹 사이트 내에 저장된다. 컨텐츠 호스팅 사이트는 컨텐츠 제공자(들)(101)에 상주하거나, 혹은 전자 디지털 컨텐츠 상점(들)(103) 및 중간 시장 파트너(도시되지 않음) 설비를 포함하는 복수의 위치에 상주할 수 있다. 컨텐츠(113) 및 키들(이후 기술함)이 암호화되어 SC 내에 패킹되므로, 전자 디지털 컨텐츠 상점(들)(103) 혹은 기타 다른 호스팅 에이전트가, 결제소로부터의 결제(clearance) 및 컨텐츠 제공자(들)(101)에 대한 통지 없이 암호해독된 컨텐츠(113)에 직접 액세스할 수 없다.

2. 전자 디지털 컨텐츠 상점(들)(103)

전자 디지털 컨텐츠 상점(들)(103)은 컨텐츠(113) 테마 프로그래밍(theme programming) 혹은 컨텐츠(113)의 전자 판매와 같은 다양한 서비스 혹은 애플리케이션을 통해 컨텐츠(113)를 마케팅하는 개체들이다. 전자 디지털 컨텐츠 상점(103)은 이들 서비스의 디자인, 개발, 사업 운용, 대금 결제, 판매, 마케팅, 세일즈를 관리한다. 온라인 전자 디지털 컨텐츠 상점(103)의 예로서, 소프트웨어의 전자적인 다운로드를 제공하는 웹사이트를 들 수 있다.

서비스 내에서, 전자 디지털 컨텐츠 상점(들)(103)은 안전한 디지털 전자 분배 시스템(100)의 특정한 기능을 구현한다. 전자 디지털 컨텐츠 상점(들)(103)은 컨텐츠 제공자(101)로부터 정보를 수집하고, 추가적인 SC들 내에 컨텐츠 및 메타데이터를 패킹하고, 이들 SC들을 서비스 혹은 애플리케이션의 일부로서 소비자 혹은 업체들에 배송한다. 전자 디지털 컨텐츠 상점(들)(103)은 보조를 위해 안전한 디지털 컨텐츠 전자 배포 시스템(100)에 의해 제공된 툴들인 메타데이터 추출, 2차 사용 조건, SC 패키징, 전자 컨텐츠 트랜잭션의 추적을 사용한다. 2차 사용 조건 데이터는 컨텐츠(113) 매수 가격, 1회 청취당 가격, 복사 인증 및 타겟 디바이스 유형, 혹은 시간부(timed-availability) 제한과 같은 소매업 제의(retail business offers)를 포함한다.

일단, 전자 디지털 컨텐츠 상점(들)(103)이 엔드 유저(들)로부터의 전자 컨텐츠(113)에 대한 유효한 요구를 완료하면, 전자 디지털 컨텐츠 상점(들)(103)은 컨텐츠(113)에 대한 암호해독 키를 소비자에게 발급(release)하도록 결제소(들)(105)에 인증할 책임을 진다. 전자 디지털 컨텐츠 상점(들)은 컨텐츠(113)를 담고 있는 SC의 다운로드를 인증하기도 한다. 전자 디지털 컨텐츠 상점(들)은 그의 로컬 사이트에 디지털 컨텐츠를 담고 있는 SC들을 호스트하고/하거나 다른 컨텐츠 호스팅 사이트의 호스팅 및 배포 설비를 활용할 것을 선택할 수 있다.

전자 디지털 컨텐츠 상점(들)은 안전한 디지털 컨텐츠 전자 배포 시스템(100)을 사용하여, 엔드 유저(들)이 가질 수도 있는 질의 또는 문제점에 대한 소비자 서비스를 제공할 수 있거나, 전자 디지털 컨텐츠 상점(들)(103)이 결제소(들)(105)에 대해 그들의 소비자 서비스 지원을 계약할 수도 있다.

3. 중간 시장 파트너(도시되지 않음)

다른 실시예에 있어서, 컨텐츠(113)를 중간 시장 파트너라 불리는 다른 업체에 안전하게 제공하기 위해 안전한 디지털 컨텐츠 전자 배포 시스템(100)이 사용될 수 있다. 이들 파트너들은 텔레비전 방송국 혹은 비디오 클럽, 라디오 방송국 혹은 레코드 클럽 등과 같이 컨텐츠(113)를 배급하는 비(非)전자적인 서비스를 제공하는 디지털 컨텐츠와 관련된 회사들을 포함할 수 있다. 이들 파트너들은 레코드 방송국, 복제국(replicator), 프로듀서들과 같은 사운드 레코딩의 제작 혹은 마케팅의 일부로서의 산물을 처리하는 다른 신뢰받은 당사자(trusted parties)를 또한 포함할 수 있다. 이들 중간 시장 파트너들은 컨텐츠(113)를 암호해독하기 위해 결제소(들)(105)로부터의 결제를 필요로 한다.

4. 결제소(들)(105)

결제소(들)(105)는 SC 내에 암호화된 컨텐츠(113)의 판매 및/또는 허가된 사용에 관련된 모든 트랜잭션의 라이센싱 인증(licensing authorization)과 레코드 보관(record keeping)을 제공한다. 결제소(들)(105)가 중간 혹은 엔드 유저(들)로부터 컨텐츠(113)를 위한 복호화 키(decryption key)에 대한 요구를 수신할 때, 결제소(들)(105)는 요구 내에 포함된 정보의 진정성(integrity) 및 신뢰성(authenticity)을 확인하고, 이 요구가 전자 디지털 컨텐츠 상점(들) 혹은 컨텐츠 제공자(들)(101)에 의해 인증되었음을 확인(verify)하고, 요구된 사용이 컨텐츠 제공자(들)(101)에 의해 규정된 컨텐츠 사용 조건에 부합한다는 것을 확인한다. 일단 이를 확인이 만족되면, 결제소(들)(105)는 요구 엔드 유저(들)에게 라이센스 SC 내에 패킹된 컨텐츠(113)에 대한 암호해독 키를 전송한다. 이 키는 단지 인증된 사용자만이 이를 인출(retrieve)할 수 있는 식으로 암호화되어 있다. 만일 엔드 유저(들)의 요구가 확인 가능하지 않거나, 완전하지 않거나, 혹은 인증되지 않으면, 결제소(들)(105)은 암호해독 키에 대한 요구를 거부한다.

결제소(들)(105)는 모든 트랜잭션들의 레코드를 유지하고, 즉시, 혹은 주기적으로, 혹은 제한된 기준으로 전자 디지털 컨텐츠 상점(들)(103) 및 컨텐츠 제공자(들)(101)과 같은 책임 있는 당사자들에게 이것을 보고한다. 이 보고는, 컨텐츠 제공자(들)(101)이 컨텐츠(113)의 판매를 보고받고, 전자 디지털 컨텐츠 상점(들)(103)이 그들의 소비자들에 대한 전자적 배송의 회계감사 실적을 획득할 수 있는 수단이 된다. 결제소(들)(105)은 또한 SC 내의 정보가 타협되었는지 혹은 컨텐츠의 사용 조건에 부합하지 않는다는 것을 검지하면, 컨텐츠 제공자(들)(101) 및/또는 전자 디지털 컨텐츠 상점(들)(103)에게 통지할 수 있다. 결제소(들)(105)는 데이터베이스의 트랜잭션 리코딩 및 저장실의 용량은 데이터마이닝 및 보고서 생성을 위해 구조화된다.

다른 실시예에 있어서, 결제소(들)(105)는 대금 환불, 전송 실패, 그리고 판매에 있어서의 실랑이와 같은 트랜잭션에 대한 소비자 지원 및 예외 처리를 제공할 수 있다. 결제소(들)(105)는 권리 관리 및 계량화에 대한 신뢰받은 관리(trusted custodian)를 제공하는, 독립적인 개체로서 동작할 수 있다. 그것은 필요에 따라 계산서 발송 및 결제(settlement)를 제공한다. 전자 결제소(들)의 예로서, 비자(Visa)/마스터카드(Mastercard)로부터의 안전한 전자 트랜잭션(Secure Electronic Transaction(SET)) 및 Secure-Bank.com이 포함된다. 한 실시예에서는, 결제소(들)(105)는 엔드 유저 장치(들)(109)에 액세스할 수 있는 웹사이트이다. 다른 실시예에서는, 결제소(들)(105)는 전자 디지털 컨텐츠 상점(들)(103)의 일부이다.

5. 엔드 유저 장치(들)(109)

엔드 유저 장치(들)(109)는 안전한 디지털 컨텐츠 전자 분배 시스템(100) 명세에 부합하는 엔드 유저 재생기 애플리케이션(195)(이후 기술함)을 담고 있는 여러 재생 장치라도 가능하다. 이들 장치들에는, PCS, 셋탑박스(IRD), 인터넷 기기들이 포함된다. 엔드 유저 재생기 애플리케이션(195)은 소프트웨어 및/또는 가전 기기(consumer electronics) 하드웨어로서 구현될 수 있다. 재생, 기록, 라이브러리 관리 기능을 수행하는 것 이외에도, 엔드 유저 재생기 애플리케이션(195)은 SC 처리를 행하여, 엔드 유저 장치(들)(109)에서의 권리 관리가 가능하도록 한다. 엔드 유저 장치(들)(109)는 디지털 컨텐츠를 담고 있는 SC들의 다운로드와 저장을 관리하고, 결제소(들)(105)로부터의 암호화된 디지털 컨텐츠 키들의 영수증을

요구하고 관리하고, 디지털 컨텐츠가 복제되거나 재생될 때마다 워터마크(들)을 처리하고, 디지털 컨텐츠(들)의 사용 조건에 부합하도록 이루어진 복제본(혹은 복제본의 삭제)의 수를 관리하고, 허가된 경우 외부 매체 혹은 휴대용 소비자 장치에 대한 복제를 수행한다. 휴대용 소비자 장치는 워터마크 내에 내장된 컨텐츠의 사용자 조건을 처리하기 위해, 엔드 유저 재생기 애플리케이션(195)의 일부분(subset)을 수행할 수 있다. 엔드 유저(들) 및 엔드 유저 재생기 애플리케이션(195)이라는 용어는 본 명세서 전반에 걸쳐, 엔드 유저 장치(들)(109)의 사용 혹은 실행을 통해 사용된다.

6. 전송 인프라(107)

안전한 디지털 컨텐츠 전자 배포 시스템(100)은 전자 디지털 컨텐츠 상점(들)(103) 및 엔드 유저 장치(들)(109)를 접속시키는 전송 네트워크와는 독립적이다. 안전한 디지털 컨텐츠 전자 배포 시스템(100)은 인터넷과 같은 점대점 분산 모델이나, 디지털 브로드캐스트 텔레비전과 같은 브로드캐스트 분산 모델을 다같이 지원한다.

여러가지 전송 인프라(107) 상의 컨텐츠(113)를 획득하고, 패키징하고, 추적은 데 동일한 툴 및 애플리케이션이 사용되기는 하지만, 선택된 인프라 및 분산 모델에 따라 서비스가 소비자에게 배송되는 형태 및 방식은 상이할 수 있다. 높은 대역폭의 인프라가 낮은 대역폭의 인프라에 비해 보다 만족할 만한 응답 속도로 양질(良質)의 디지털 컨텐츠를 배송할 수 있으므로, 전송되는 컨텐츠(113)의 질은 상이할 수 있다. 점대점 분산 모델을 위해 디자인된 서비스 애플리케이션은 또한 브로드캐스트 분산 모델을 지원하도록 변형될 수 있다.

C. 시스템 사용

안전한 디지털 컨텐츠 전자 분배 시스템(100)은, 소비자이건 업체이건 상관 없이, 엔드 유저 장치(들)109)에 대해 컨텐츠(113)의 양질의 전자적인 복제가 가능하도록 하며, 컨텐츠(113)의 규제 및 사용 추적을 가능하게 한다.

안전한 디지털 컨텐츠 전자 배포 시스템(100)은 신규한 혹은 기존의 분배 채널을 모두 사용하여 다양한 소비자 및 기업간(business-to-busiress) 서비스에 대해 적용될 수 있다. 각각의 특정한 서비스는 안전한 디지털 컨텐츠 전자 배포 시스템(100)의 권리 관리 특성을 통해 실현되는 상이한 재정적인 모델(financial model)을 사용할 수 있다. 도매 혹은 소매 구입, 1회 청취당 대금 지불, 구독 서비스, 복제/비복제 제한, 혹은 재분배와 같은 모델들이 결제소(들)(105) 및 엔드 유저 재생기 애플리케이션(195) 복제 방지 특성의 권리 관리를 통해 구현될 수 있다.

안전한 디지털 컨텐츠 전자 분배 시스템(100)은, 전자 디지털 컨텐츠 상점(들)(10) 및 중간 시장 파트너에게, 컨텐츠(113)를 판매하는 서비스를 창조하는 데 있어서 커다란 융통성을 허용한다. 동시에, 안전한 디지털 컨텐츠 전자 분배 시스템(100)은, 컨텐츠 제공자(들)(101)에게, 컨텐츠(113)의 리이센싱에 대해 그들이 적절한 보상을 받을 수 있도록 디지털 자산이 보호되고 계량화된다는 것에 대한 일정한 수준의 보장을 제공한다.

II. 안전한 디지털 컨텐츠 전자 배포 시스템에 대한 암호화 개념 및 그 적용

안전한 디지털 컨텐츠 전자 배포 시스템(100) 내에서의 라이센스 제어(License Control)는 암호화의 사용에 기초한다. 이 절에서는 본 발명의 기본적인 암호화 기법을 소개한다. 공개 키 암호화(public key encryption), 대칭 키 암호화(symmetric key encryption), 디지털 서명, 디지털 워터마크, 디지털 인증(digital certificates)의 사용이 알려져 있다.

A. 대칭형 알고리즘

안전한 디지털 컨텐츠 전자 배포 시스템(100)에서, 컨텐츠 제공자(들)(101)는 대칭형 알고리즘을 사용하여 컨텐츠를 암호화한다. 데이터를 암호화하고 암호해독하는 데 동일한 키가 사용되므로, 이들을 대칭형 알고리즘이라 부른다. 데이터 송신자와 메시지 수신자는 키를 공유하여야 한다. 공유된 키는 본 명세서에서 대칭 키라 부른다. 안전한 디지털 컨텐츠 전자 배포 시스템(100) 구조는 특별한 구현예를 위해 선택된 특정의 대칭형 알고리즘과는 무관하다.

일반적인 대칭형 알고리즘은 DES, RC2, RC4가 있다. DES와 RC2는 블럭 사이퍼(block ciper)이다. 블럭 사이퍼는 한 번에 한 블럭의 데이터비트들을 사용하여 데이터를 암호화한다. DES는 미국 정부의 공식적인 암호화 표준으로서, 64 비트 블럭 크기를 가지며, 56 비트의 키를 사용한다. 단순한 DES로 얻을 수 있는 보안도(security)를 증가시키기 위해 트리플 DES가 흔히 사용된다. RSA 데이터 시큐리티 사(RSA Data Security)는 RC2를 디자인하였다. RC2는 가변키 크기 사이퍼를 사용하며, 64 비트 크기의 블럭을 갖는다. 역시 RSA 데이터 시큐리티사에 의해 디자인된 RC4는 가변 키 크기 스트림 사이퍼이다. 한 번에 하나의 데이터 비트에 대해 하나의 스트림 사이퍼가 동작한다. RSA 데이터 시큐리티사는 출력 바이트마다 RC에 대해 8 내지 16 머신 오퍼레이션이 필요하다고 주장한다.

IBM은 SEAL이라 불리는 고속 알고리즘을 디자인하였다. SEAL은 가변 길이 키를 사용하는 스트림 알고리즘으로서, 32 비트 프로세서에 대해 최적화되었다. SEAL은 데이터 바이트마다 5 번의 기본적인 머신 인스트럭션을 필요로 한다. 사용된 160 비트 키가 내부 테이블로 미리 전처리되었다고 하면, 50 MHZ의 486 기반 컴퓨터는 SEAL 코드를 7.2 메가바이트/초의 속도로 동작시킨다.

마이크로소프트사는 CryptoAPI 개괄 문서에서, 암호화 성능 벤치마크의 결과를 보고하였다. 이들 결과들은 윈도우즈 NT 4.0에 의한 120 MHZ의 펜티엄 기반 컴퓨터 상에서 실행되는 마이크로소프트의 CryptoAPI

를 사용한 애플리케이션에 의해 얻어졌다.

사이퍼	키 크기	키 설정 시간	암호화 속도
DES	56	460	1,138,519
RC2	40	40	286,888
RC4	40	151	2,177,723

B. 공개 키 알고리즘

안전한 디지털 컨텐츠 전자 배포 시스템(100)에 있어서, 대칭 키와 기타 작은 데이터 조각들이 공개 키를 사용하여 암호화된다. 공개 키 알고리즘은 두 개의 키를 사용한다. 이들 두 개의 키들은, 하나의 키에 의해 암호화된 데이터는 다른 키에 의해서만 암호해독될 수 있도록 수학적으로 연관되어 있다. 키들의 소유자는 하나의 키를 비밀로 두고(비밀 키) 두 번째 키(공개 키)를 공개적으로 유통시킨다.

공공키 알고리즘을 이용한 기밀 메시지의 전송을 보장하기 위해서는, 수신자의 공공키를 이용하여 메시지를 암호화해야만 한다. 관련된 개인 키를 가지는 수신자만이 메시지를 암호 해독할 수 있다. 또한, 공공키 알고리즘은 디지털 서명을 생성하는데 이용된다. 개인키는 그 목적을 위해 이용된다. 다음 섹션이 디지털 서명에 대한 정보를 제공한다.

대부분 공통적으로 이용되는 공공키 알고리즘으로 RSA 공공키 암호가 있다. 산업에서 그것은 실질적인 공공키 표준으로 되었다. 또한, 암호화 및 디지털 서명을 보다 잘 수행하는 다른 알고리즘으로 ElGmal 및 RabinOI 있다. RSA는 가변-키 길이 암호이다.

공공키 알고리즘보다 대칭 키 알고리즘이 더 빠르다. 소프트웨어에 있어서, 일반적으로 DES는 RAS보다 100배 더 빠르다. 이러한 이유 때문에, 벌크(bulk) 데이터를 암호화하는데 RSA는 이용되지 않는다. RSA 데이터 안전(Data Security)의 툴키트(toolkit) BSAFE 3.0은 512-비트 모듈러스를 가진 21.6킬로비트/초 및 1024-비트 모듈러스를 가진 7.4킬로비트/초의 개인 키 연산(개인키를 사용한 암호화 또는 암호 해독) 처리량을 가진다

C. 디지털 서명

안전한 디지털 컨텐츠 전자 배포 시스템(100)에 있어서, SC(들) 발행자는 그것을 디지털적으로 서명함에 의해 SC(들)의 무결성을 보호한다. 일반적으로, 메시지의 디지털 서명을 생성하기 위해, 우선적으로 메시지 소유자는 메시지 다이제스트를 연산하고, 그 다음에 소유자의 개인 키를 이용하여 메시지 다이제스트를 암호화한다. 메시지는 그의 서명과 함께 배포된다. 메시지 수신자는, 우선적으로, 메시지 다이제스트를 복구하기 위해 메시지 소유자의 공공키를 이용하여 서명을 암호 해독함으로서 디지털 메시지를 확인할 수 있다. 그 다음, 수신자는 수신된 메시지의 다이제스트를 계산하고, 그것을 복구된 것과 비교한다. 배포중에 메시지가 변경되지 않은 상태라면, 계산된 다이제스트 및 복구된 다이제스트는 동일해야만 한다.

안전한 디지털 컨텐츠 전자 배포 시스템(100)에 있어서, SC(들)가 여러개에 데이터 부분을 포함하기 때문에, 다이제스트는 부분마다 연산되고, 개략 다이제스트가 연결 부분 다이제스트에 대해 연산된다. 개략 다이제스트는 SC(들) 발행자의 개인 키를 이용하여 암호화된다. 암호화된 개략 다이제스트는 SC(들)에 대한 발행자의 디지털 서명이다. 부분 다이제스트 및 디지털 서명은 SC(들)의 몸체에 포함된다. SC(들)의 수신자는 수신된 디지털 서명 및 부분 다이제스트에 의해 그 부분과 SC(들)의 무결성을 확인할 수 있다.

메시지 다이제스트를 계산하는데 일 방향 해쉬(hash) 알고리즘이 이용된다. 해쉬 알고리즘은 가변 길이 입력 메시지를 취하고, 그것을 고정 길이 스트링(string)의 메시지 다이제스트로 변환한다. 일 방향 해쉬 알고리즘은 단지 일 방향으로만 작용한다. 즉, 입력 메시지에 대한 다이제스트를 계산하기는 쉽지만, 그 다이제스트로부터 입력 메시지를 생성하기는 매우 어렵다(계산을 통해 실행될 수 없다). 일방향 해쉬 함수의 성질로 인해, 메시지의 지문으로서 메시지 다이제스트를 메시지 지문으로 여길 수 있다.

보다 일반적인 일방향 해쉬 함수는 RSA 데이터 안전으로 부터의 MD5 및 US NITS(National Institute of Technology and Standards)에 의해 고안된 SHAOI다.

D. 디지털 인증

디지털 인증은, 사람 또는 디지털적으로 서명된 메시지를 전송한 엔티티(entity)의 일치 여부를 인증하거나 확인하는데 이용된다. 인증은, 공공키를 사람 또는 엔티티와 연계시키는 인증국에 의해 발행된 디지털 서류이다. 인증은 공공키, 사람 또는 엔티티의 이름, 만료일, 인증국의 이름, 및 다른 정보를 포함한다. 또한, 인증은 인증국의 디지털 서명을 포함한다.

엔티티(또는 사람)가 그의 개인키로 서명되고 그의 디지털 인증을 수반한 메시지를 전송하면, 메시지 수신자는 인증으로부터의 엔티티 이름을 이용하여 그 메시지를 수신할지의 여부를 결정한다.

안전한 디지털 컨텐츠 전자 배포 시스템(100)에 있어서, 엔드 유저 장치(109)에 의해 발행된 것을 제외한 각 SC(들)는, SC(들) 생성기의 인증을 포함한다. 엔드 유저 장치(109)는, 많은 엔드 유저들이 굳이 인증을 획득하거나, 허위 인증국들에 의해 발행된 인증을 가질려고 하지 않기 때문에, 그들의 SC(들)에 인증을 포함할 필요가 없다. 안전한 디지털 컨텐츠 전자 배포 시스템(100)에 있어서, 결제소(105)는 전자 디지털 컨텐츠 상점(103)을 위해 선택적으로 인증을 발행한다. 이에 따라, 엔드 유저 장치(109)는, 전자 디지털 컨텐츠 상점(103)이 안전한 디지털 전자 배포 시스템(100)에 의해 인증되는 것을 독자적으로 확인할 수 있게 된다.

E. SC(들)의 그래픽 표시에 대한 가이드.

이 명세서는 도면을 이용하여, 암호화부, 비 암호화부, 암호화 키 및 인증을 나타내는 SC(들)를 그래픽으로 표시한다. 도 2를 참조하면, SC(들)(200)에 대한 도면이 예시된다. 다음의 심볼들이 SC(들) 도면에 이

용된다. 키(201)은 공공키 또는 개인키이다. 예를들어 결제소에 대한 CLRNGHR와 같은 키의 이름은 키 소유자를 나타낸다. 핸들 내부의 PB는 그것이 개인키임을 나타내며, 따라서 키(201)는 결제소 공공키이다. 핸들 내부의 PV는 그것이 공공키임을 나타낸다. 다이아몬드 형상은 엔드 유저 디지털 서명(202)이다. 머리 글자들은, 개인키가 서명을 생성하는데 이용되었음을 나타내며, 예를들면 아래의 표에서 EU는 엔드 유저 디지털 서명이다. 대칭 키(203)는 컨텐츠를 암호화하는데 이용된다. 암호화 대칭키 객체(204)는 CLRNGH의 PB로 암호화된 대칭키(203)를 포함한다. 직사각형 상단 가장자리상의 키는 객체의 암호화에 이용된 키이다. 직사각형 내의 심볼 또는 텍스트는 암호화된 객체(이 경우에는 대칭키)를 나타낸다. 다른 암호화된 객체, 본 실시예에서는 트랜잭션 ID 암호화 객체(205)가 도시된다. 또한, 아래에 설명된 바와 같이 컨텐츠 라이센싱 관리를 위한 사용 조건(206)이 있다. SC(들)(200)는 사용 조건(206), 트랜잭션 ID 암호화 객체(205), 어플리케이션 ID 암호화 객체(207) 및 암호화 대칭 키 객체(204)를 포함하며, 그 모두는 엔드-유저 디지털 서명(202)으로 서명된다.

아래의 표는 SC(들)의 서명자를 식별하는 머리 글자를 나타낸다.

머리 글자	구성 요소
CP	컨텐츠 제공사(들)(101)
MS	전자 디지털 컨텐츠 상점(들)(103)
HS	컨텐츠 호스팅 사이트(들)(111)
EU	엔드 유저 장치(들)(109)
CH	결제소(들)(105)
CA	인증국(들)(도시되지 않음)

F. 안전한 컨테이너 암호화의 예

아래의 표 및 다이어그램은 SC(들)로부터 정보를 생성하고 복구하는데 이용되는 암호화 및 암호 해독에 대한 개요를 제공한다. 이 프로세스 개요에서 생성되고 암호 해독된 SC(들)는 일반적인 SC(들)이다. 그것은 안전한 디지털 컨텐츠 전자 배포 시스템(100)에 있어서 권리 관리에 이용되는 특정한 SC(들) 타입을 전혀 나타내지 못한다. 프로세스는 암호화 프로세스에 대한 도 3에 도시된 단계를 포함한다.

도 3의 암호화 프로세스에 대한 프로세스 흐름

단계 프로세스

301 송신자는 랜덤한 대칭키를 생성하고 그것을 컨텐츠를 암호화하는데 이용한다.

302 송신자는 암호화된 컨텐츠에 해쉬 알고리즘을 적용하여 컨텐츠 다이제스트를 생성한다.

303 송신자는 수신자의 공공키를 사용하여 대칭키를 암호화하며, PB PECPNT는 수신자의 공공키를 지칭한다.

304 송신자는 암호화된 대칭키에 단계2에서 이용된 것과 동일한 해쉬 알고리듬을 적용하여 대칭키 다이제스트를 생성한다.

305 송신자는 컨텐츠 다이제스트 및 대칭키 다이제스트의 연결에 단계2에서 이용된 것과 동일한 해쉬 알고리즘을 적용한다.

306 송신자는 송신자의 개인키로 SC(들) 다이제스트를 암호화하여, SC(들)에 대한 디지털 서명을 생성한다. PV SENDER는 송신자의 개인키를 지칭한다.

307B 송신자는 암호화 컨텐츠와, 암호화 대칭 키와, 컨텐츠 다이제스트와, 대칭키 다이제스트와, 송신자 인증 및 SC(들) 서명을 포함하는 SC(들) 파일을 생성한다.

307A 송신자는 안전한 통신을 개시하기 전에 인증국으로부터 인증을 얻어야만 한다. 인증에 있어서, 인증국은 송신자의 공공키와 송신자의 이름을 포함하고, 그것을 서명한다. PV CAUTHR은 인증국의 개인키를 지칭한다. 송신자는 수신자에게 SC(들)를 전송한다.

도 4의 암호 해독에 대한 프로세스 흐름

단계 프로세스

408 수신자는 SC(들)를 수신하고 그의 일부를 분리한다.

409 수신자는, 그것을 인증국의 공공키로 암호 해독하여 송신자의 인증에 있는 디지털 서명을 확인한다. 인증 디지털 서명이 유효하다면, 수신자는 인증으로부터 송신자의 공공키를 획득한다.

410 수신자는 수신자의 공공키를 이용하여 SC(들) 디지털 서명을 암호 해독한다. PB SENDER는 송신자의 공공키를 지칭한다.

411 수신자는, 수신된 컨텐츠 다이제스트 및 암호화 키 다이제스트에 송신자에 의해 사용된것과 동일한 해쉬 알고리듬을 적용하여 SC(들) 다이제스트를 계산한다.

412 수신자는 계산된 SC(들) 다이제스트와 송신자의 디지털 서명으로부터 복구된 것을 비교한다. 그들이 동일하다면, 수신자는 수신된 다이제스트가 변경되지 않았음을 확신하여 암호 해독 프로세스를 계속 진행한다. 그들이 동일하지 않다면, 수신자는 SC(들)를 폐기하고 송신자에게 통지한다.

413 수신자는 암호화 대칭 키에 단계 411에서 사용된것과 동일한 해쉬 알고리즘을 적용하여 대칭키 다이제스트를 계산한다.

414 수신자는 계산된 대칭키 다이제스트와 SC(들)에서 수신된 것을 비교한다. 그들이 동일하다면, 수신자는 암호화 대칭키가 변경되지 않았음을 인식한다. 수신자는 암호 해독 프로세스를 계속 진행한다. 만약 유효하지 않다면, 수신자는 SC(들)를 폐기하고 송신자에게 통보한다.

415 수신자는 암호화 컨텐츠에 단계 411에서 사용된 것과 동일한 해쉬 알고리즘을 적용하여 컨텐츠 다이제스트를 계산한다.

416 수신자는 계산된 컨텐츠 다이제스트와 SC(들)에서 수신된 것을 비교한다. 그것이 동일하다면, 수신자는 암호화 컨텐츠가 변경되지 않았음을 인식한다. 수신자는 암호 해독 프로세스를 계속 진행한다. 유효하지 않다면, 수신자는 SC(들)를 폐기하고 송신자에게 통보한다.

417 수신자는 수신자의 개인키를 이용하여 암호화 대칭키를 암호 해독한다. 이에 따라 대칭키가 복구된다. PV RECPNT는 수신자의 개인키를 지칭한다.

418 수신자는 대칭키를 사용하여 암호화 컨텐츠를 암호 해독한다. 이에 따라 컨텐츠가 복구된다.

III. 안전한 디지털 컨텐츠 전자 배포 시스템 흐름

안전한 전자 디지털 컨텐츠 배포 시스템(100)은, 상이한 시스템 참가자에 의해 사용되는 여러 가지 구성요소를 포함한다. 이러한 참가자는 컨텐츠 제공자(들)(101), 전자 디지털 컨텐츠 상점(들)(103), 엔드 유저 장치(들)(109)를 통한 엔드 유저(들) 및 결제소(들)(105)를 포함한다. 상위 레벨 시스템 흐름이 안전 디지털 컨텐츠 전자 배포 시스템(100)의 개요로서 이용된다. 아래에 약술된 이 흐름은 그것이 시스템(100)을 전체적으로 이용하는 것에 따라 컨텐츠를 추적한다. 추가적으로, 그것은, 구매, 언록킹 및 컨텐츠(113)의 사용에 대한 트랜잭션을 실행하기 위해 참가자에 의해 사용된 단계들를 약술한다. 시스템 흐름에서 작성된 몇가지 가설은 다음을 포함한다.

- 이것은 디지털 컨텐츠 서비스(PC에 대한 점대점 인터페이스)에 대한 시스템 흐름이다.
- 컨텐츠 제공자(들)(101)는 (예를 들어 뮤직 오디오와 같이) PCM의 압축되지 않은 포맷으로 오디오 디지털 컨텐츠를 제출한다.
- 컨텐츠 제공자(들)(101)는 ODBC 컴플라이언트(compliant) 데이터 베이스에 있는 메타 데이터를 가지거나, 컨텐츠 제공자(들)(101)는 컨텐츠 정보 프로세싱 서브시스템에 직접 데이터를 입력하거나 또는 규정된 ASCII 파일 포맷으로 데이터를 제공할 것이다.
- 전자 디지털 컨텐츠 상점(들)에 의해 재정적인 조정이 실행된다
- 컨텐츠(113)는 단일 컨텐츠 호스팅 사이트(들)(11)에서 호스트된다.

이러한 가설은 디지털 컨텐츠, 예를들어 음악, 비디오 및 프로그램의 정확한 본질을 수용하도록 변경될 수 있으며 그리고 전자 배포 시스템이 방송함을 당업자라면 알 수 있을 것이다.

다음은 도 1 에 도시된 프로세스 흐름이다.

단계 프로세스

121 압축되지 않은 PCM 오디오 파일이, 컨텐츠 제공자(들)(101)에 의해 컨텐츠(113)로서 제공된다. 그의 파일 이름은 컨텐츠(113)에 대한 컨텐츠 제공자(들)(101)의 단일 식별자와 함께 작업 흐름 관리자(154) 툴로 입력된다.

122 메타데이터는 컨텐츠(113)에 대한 컨텐츠 제공자(들)의 단일 식별자를 이용하는 컨텐츠 정보 프로세싱 서브 시스템과 데이터 베이스 맵핑 템플릿(Database Mapping Template)에 의해 제공된 정보에 의해 컨텐츠 제공자(들)의 데이터 베이스(160)로부터 포획된다.

123 작업 흐름 관리자 툴(154)은 컨텐츠 제공자(들)(101)에 있는 획득 및 준비 프로세스를 통해 컨텐츠 흐름을 지향시키는 데 이용된다. 또한 그것은 임의 시간에 시스템에서 컨텐츠 견본의 상태를 추적하는 데 이용될 수 있다.

124 컨텐츠(113)에 대한 사용 조건이 컨텐츠 정보 프로세싱 서브시스템으로 입력되는데, 이는 수동 또는 자동으로 실행될 수 있다. 이러한 데이터는 카피 제한 룰 및 필요하다고 여기는 다른 비즈니스 룰을 포함한다. 모든 메타데이터 입력은 데이터에 대한 오디오 프로세싱과 나란히 발생할 수 있다.

125 워터마킹 툴은, 컨텐츠 제공자(들)(101)가 컨텐츠를 식별하는데 필요하다고 여기는 컨텐츠(113)의 데이터를 감추는데 이용된다. 이것은, 그것이 포획되었던 때, 그것이 (이 컨텐츠 제공자(들)(101)로부터) 제공되었던 곳, 또는 컨텐츠 제공자(들)(101)에 의해 특정된 임의의 다른 정보를 포함한다.

- 컨텐츠 프로세싱 툴(125)은 지원된 상이한 압축 레벨에 필요한 컨텐츠(113)에 대해 등화, 다이나믹 조정 및 재 샘플링을 실행한다.
- 컨텐츠(113)는 컨텐츠 프로세싱 툴(125)을 사용하여 원하는 압축 레벨로 압축된다. 그 다음, 압축이 필요한 레벨의 컨텐츠(113) 품질을 생성함을 확인하기 위해 컨텐츠(113)가 재생될 수 있다. 필요할 경우, 등화, 다이나믹 조정, 압축 및 재생 품질 검사를 원하는 만큼 여러번 할 수 있다.
- 컨텐츠(113)와 그의 메타데이터 서브셋은 SC 포장기에 의해 대칭키로 암호화된다. 그다음 이 툴은 결제소(들)(105)의 공공키를 이용하여 키를 암호화하여 암호화 대칭키를 생성한다. 이 키는 컨텐츠(113)의 안전을 포함하지 않는 곳이라면 어디든지 전송될 수 있는데, 이는 그것을 암호 해독할 수 있는 유일한 엔티티가 결제소(들)(105)이기 때문이다.

126 암호화 대칭키, 메타데이터 및 컨텐츠(113)에 대한 다른 정보는 SC 포장기 툴(152)에 의해 메타데이터 SC로 포장된다.

127 그 다음, 암호화 컨텐츠(113) 및 메타데이터는 컨텐츠 SC로 포장된다. 이 시점에서, 컨텐츠(113) 및 메타데이터상의 프로세싱이 완료된다.

128 컨텐츠 지불 툴(도시되지 않음)을 이용하여 메타 데이터 SC(들)를 컨텐츠 프로모션 웹 사이트(156)에 전송한다.

129 컨텐츠 지불 툴은 컨텐츠 SC(들)를 컨텐츠 호스팅 사이트(들)(111)에 제공한다. 컨텐츠 호스팅 사이트(들)는 컨텐츠 제공자(들)(101)와, 결제소(들)(105) 또는 컨텐츠 호스팅 전용의 특정 위치에 거주할 수 있다. 이 사이트에 대한 URL은 메타 데이터SC에 부가되었던 메타 데이터의 일부이다.

130 컨텐츠 프로모션 웹 사이트(156)는 전자 디지털 컨텐츠 상점(들)(103)에게 시스템(100)에 부가된 새로운 컨텐츠(113)를 통보한다.

131 컨텐츠 획득 툴을 사용하여, 전자 디지털 컨텐츠 상점(들)(103)은 그들이 팔기를 원하는 컨텐츠에 대응하는 메타데이터 SC들을 다운로드한다.

132 전자 디지털 컨텐츠 상점(들)(103)은 컨텐츠 획득 툴을 사용하여, 그들이 컨텐츠(113)를 프로모션하는데 이용하기를 바라는 메타데이터SC들로 부터 임의의 데이터를 추출한다. 이 메타데이터의 일부에 대한 억세스는 보장될 수 있으며, 원한다면 요금 청구될 수도 있다.

133 이 전자 디지털 컨텐츠 상점(들)(103) 특유의 컨텐츠(113)에 대한 사용 조건이 컨텐츠 획득 툴을 이용하여 입력된다. 이 사용 조건은 컨텐츠(113)의 상이한 압축 레벨에 대한 카피/플레이 제한 및 소매 가격을 포함한다.

134 전자 디지털 컨텐츠 상점(들)(103) 특유의 사용 조건 및 원래의 메타데이터 SC(들)는 SC 포장기 툴에 의해 공급자 SC로 포장된다.

135 전자 디지털 컨텐츠 상점(들)(103) 웹 사이트가 갱신된 후, 웹을 서핑(surfing)하는 엔드 유저(들)는 컨텐츠(113)를 이용할 수 있다.

136 엔드 유저가 구매하기를 원하는 컨텐츠(113)를 발견할 경우, 그들은 음악 아이콘(icon)과 같은 컨텐츠 아이콘을 클릭하고, 아이템(item)은 전자 디지털 컨텐츠 상점(들)(103)에 의해 유지되는 그/그녀의 쇼핑 카트(shopping cart)에 부가된다. 엔드 유저가 쇼핑을 끝마치면, 프로세싱에 대한 전자 디지털 컨텐츠 상점(들)(103)에게 구매 요청서를 제출한다.

137 전자 디지털 컨텐츠 상점(들)(103)은 신용 카드 결제 기관과 상호 작용하여 그들이 당일 날 거래했던 것과 동일한 방식으로 펀드(fund)를 예약한다.

138 일단 전자 디지털 컨텐츠 상점(들)(103)이 신용 카드 결제 기관으로부터 신용 카드 인증 번호를 수신하면, 전자 디지털 컨텐츠 상점은 이 번호를 데이터베이스에 저장하고, SC 포장기 툴을 작동시켜 트랜잭션 SC를 형성한다. 이 트랙잭션 SC는, 엔드 유저가 구입했던 컨텐츠(113)에 대한 공급자 SC들, 전자 디지털 컨텐츠 상점(들)(103)로 되돌아가서 추적될 수 있는 트랜잭션 ID, 엔드 유저(들)를 식별하는 정보, 압축 레벨, 사용 조건, 및 구입된 노래에 대한 가격 리스트 모두를 포함한다.

139 이 트랙잭션 SC는 엔드 유저 장치(들)(109)에 전송된다.

140 트랙잭션 SC가 엔드 유저 장치(들)(109)에 도달하면, 트랜잭션 SC를 개관하고 엔드 유저의 구매를 인식하는 엔드 유저 플레이어 어플리케이션(195)이 시작된다. 엔드 유저 플레이어 어플리케이션(195)은 개별적인 공급자 SC들을 개관하고, 다른 실시예에서는, 사용자에게 다운 로드 시간의 추정치를 통보한다. 그다음, 사용자에게 그들이 컨텐츠(113)를 다운로드하기를 원하는 시점을 지정할 것을 요청한다.

141 엔드 유저(들)가 다운로드를 요청했던 시간에 근거하여, 엔드 유저 플레이어 어플리케이션(195)은 작동을 시작하고, 다른 것들 사이에 컨텐츠(113)와 트랜잭션 ID 및 엔드 유저(들) 정보에 대한 암호화 대칭키를 포함시키는 지시 SC를 형성함에 의해 다운로드 프로세스를 시작한다.

142 이 지시 SC는 프로세스를 위해 결제소(들)(105)에 전송된다.

143 결제소(들)(105)는 지시 SC를 수신하고 그것을 개관하며, 변조된 데이터가 없음을 확인한다. 결제소(들)(105)는 엔드 유저(들)에 의해 구입된 사용 조건을 허가한다. 이 사용 조건은 컨텐츠 제공자(들)(101)에 의해 지정된 사용 조건을 따라야 한다. 이 정보는 데이터베이스에 기록된다.

144 일단 모든 체크가 완료되면, 암호화 대칭키는 결제소(들)(105)의 개인키를 이용하여 암호 해독된다. 그 다음 대칭키는 엔드 유저(들)의 공공키를 이용하여 암호화된다. 이러한 새로운 암호화 대칭키는 SC 포장기에 의해 라이센스 SC로 포장된다.

145 라이센스 SC는 엔드 유저(들)에 전송된다.

146 엔드 유저 장치(들)(109)에서 라이센스 SC를 수신하면, 컨텐츠 SC가 다운로드될 때 까지 라이센스 SC는 메모리에 저장된다.

147 엔드 유저 장치(들)(109)는 컨텐츠 호스팅 기관(111)에게, 구입된 컨텐츠(113)에 대응하는 라이센스 SC를 전송할 것으로 요청한다.

148 컨텐츠(113)는 유저 엔드 장치(들)(109)에 전송된다. 수신시에, 컨텐츠(113)는 대칭키를 이용하여 엔드 유저 장치(들)에 의해 암호 해독된다.

IV. 권리 관리 구조 모델

A. 구조층 기능

도 5는 안전한 디지털 컨텐츠 전자 배포 시스템(100)의 권리 관리 구조에 대한 블록도이다. 구조적으로,

4개의 층, 즉 라이센스 제어 층(501)과, 컨텐츠 식별층(503)과, 컨텐츠 사용 제어층(505) 및 컨텐츠 포맷팅 층(507)은 안전한 디지털 컨텐츠 전자 배포 시스템(100)을 나타낸다. 각층의 전반적인 기능적 목적 및 각층에 대한 개인키 기능이 아래에 설명된다. 각 층에 있어서의 기능은 다른 층의 기능과 전혀 별개이다. 넓은 제한내에서, 각층의 기능은 다른층의 기능성에 영향을 미치지 않은 유사한 기능으로 대치될 수 있다. 명백히, 하나의 층으로 부터의 출력이 이웃층에서 수용할 수 있는 포맷 및 시멘틱(semantic)을 만족시킬 필요가 있다.

라이센스 제어 층(501)은 다음을 보증한다.

- 디지털 컨텐츠는 배포동안에 불법 방해 및 변경으로부터 보호된다.

- 컨텐츠(113)는 합법적인 컨텐츠 소유자로부터 발생하며, 인가받은 배포자, 즉 전자 디지털 컨텐츠 상점(들)(103)에 의해 배포된다.

- 디지털 컨텐츠 구매자는 적정하게 인가받은 어플리케이션을 가진다.

- 구매자 또는 엔드 유저(들)가 이용할 수 있도록 컨텐츠(113)의 사본이 작성되기 전에 배포자는 구매자에 의해 지불된다.

- 트랜잭션의 기록은 기록 목적을 보존한다.

컨텐츠 식별층(503)으로 인해 저작권을 확인할 수 있으며, 컨텐츠 구매자의 신원을 알수 있다. 컨텐츠의 저작권 정보 및 컨텐츠 구매자의 신원으로 인해, 임의의 인증되거나 그렇지 않은 컨텐츠(113)의 사본을 소오스 추적할 수 있다. 따라서, 컨텐츠 식별층(503)은 표절과 다투기 위한 수단을 제공한다.

컨텐츠 사용 제어층(505)은 컨텐츠(113)의 사본이 상점 사용 조건(519)에 따라 구매자 장치에서 사용되도록 한다. 상점 사용 조건(519)은 플레이 수 및 컨텐츠(113)에게 허용된 로컬 사본을 지정하고, 컨텐츠(113)가 외부 휴대 장치에 기록될 것인지를 지정한다. 컨텐츠 사용 제어층(505)의 기능은 컨텐츠의 카피/플레이 사용의 진로를 유지하고 카피/플레이 상태를 갱신하는 것이다.

컨텐츠 포멧팅 층(507)은, 컨텐츠 소유자의 설비에 있는 그의 고유의 표시에서, 안전한 디지털 컨텐츠 전자 배포 시스템(100)의 서비스 특징 및 배포 수단과 일치하는 형태로의, 컨텐츠(113)의 포맷 변환을 고려한다. 변환 프로세싱은 압축 인코딩과 그와 관련된 사전 프로세싱, 예를들어 주파수 등화 및 크기 다이나믹 조정을 포함한다. 구매자 측에서, 오디오 컨텐츠(113)에 대해, 수신 컨텐츠(113)는 재생에 적당한 포맷을 이루고 휴대 장치로 전달하도록 처리될 필요가 있다.

B. 기능 분할 및 흐름

권리 관리 구조 모델은 도 5에 도시되며, 여기에서는 안전한 디지털 컨텐츠 전자 배포 시스템(100)으로 이루어진 작동 구성 요소 및 각 층의 키 기능으로 구조층을 맵핑하는 것을 설명한다.

1. 컨텐츠 포맷팅 층(507)

컨텐츠 포맷팅 층(507)과 관련된 일반적인 기능으로, 컨텐츠 제공자(들)(101)에는 컨텐츠 사전 프로세싱(502) 및 압축(511)이 있으며, 엔드 유저 장치(들)(109)에는 컨텐츠 디스크램블링 및 압축 해제(515)가 있다. 사전 프로세싱 및 특정 기능의 예에 대한 필요성은 상술한 바와 같다. 컨텐츠 압축(511)은 컨텐츠(113)의 파일 크기 및 전송 시간을 줄이는데 이용된다. 컨텐츠(113) 타입에 적당한 압축 알고리즘 및 전송 매체는 안전한 디지털 컨텐츠 전자 배포 시스템(100)에 이용될 수 있다. 음악에 있어서, MPEG4, 돌비 AC-2 및 AC-3, 소니 적응적 변환 코딩(ATRAC) 및 저 비트 속도 알고리즘은 전형적으로 이용되는 몇가지 압축 알고리즘이다. 컨텐츠(113)는 엔드 유저 장치(들)(109)에 압축 형태로 저장되어 저장 크기 요건을 줄인다. 그것은 활성 재생동안에 압축 해제된다. 또한, 활성 재생동안에 디스크램블링이 실행된다. 스크램블링의 목적 및 타입은 나중의 컨텐츠 사용 제어 층(505)의 설명중에 언급된다.

2. 컨텐츠 사용 제어층(505)

컨텐츠 사용 제어층(505)은 엔드 유저 장치(들)에서 컨텐츠(113) 사용에 부과되는 조건들 또는 제한들의 사양 및 실시를 허용한다. 조건들은 컨텐츠(113)에 대해 허용된 재생(play)의 수, 컨텐츠(113)의 2차 카피가 허용되는지의 여부 및 컨텐츠(113)가 외부 휴대형 장치에 카피될 수 있는지의 여부를 지정할 수 있다. 컨텐츠 제공자(들)(101)는 허용가능한 사용 조건(517)을 설정해서 그룹을 SC(라이센트 제어층(517) 섹션 참조)의 전자 디지털 컨텐츠 상점(들)(103)에게로 전송한다. 전자 디지털 컨텐츠 상점(들)(103)은 컨텐츠 제공자(들)(101)에 의해 설정된 최초의 조건들을 유효화하지 않는 한 사용 조건(517)을 늘리거나 줄일 수 있다. 그리고 나서, 전자 디지털 컨텐츠 상점(들)(103)은 모든 상점 사용 조건(519)(SC내에 있는)을 엔드-유저 장치(들)(109) 및 결제소(들)(105)에게로 전송한다. 결제소(들)(105)은 엔드-유저 장치(들)(109)에 대한 컨텐츠(113) 해제를 인증하기 전에 사용 조건 유효성 확인(521)을 수행한다.

컨텐츠 사용 조건(517)의 실시는 엔드-유저 장치(들)(109)의 컨텐츠 사용 제어층(505)에 의해 수행된다. 첫째, 엔드-유저 장치(들)(109)에서 컨텐츠 식별층(503)으로부터의 컨텐츠(113) 카피 수신시 컨텐츠(113)를 초기 카피/재생 허용을 나타내는 카피/플레이 코드(523)로 표시한다. 둘째, 재생기 애플리케이션(195)은 컨텐츠(113)를 암호로 스크램블해서 그것을 엔드-유저 장치(들)(109)에 저장한다. 재생기 애플리케이션(195)은 각각의 컨텐츠 항목에 대해 스크램블링 키를 발생하며, 키는 암호화되어 엔드-유저 장치(들)(109)에 은닉된다. 그리고 나서, 엔드-유저 장치(들)(109)가 카피 또는 재생을 위해 컨텐츠(113)를 액세스할 때마다, 엔드-유저 장치(들)(109)는 카피/재생 코드를 검증해서 컨텐츠(113)의 디스크램블링 및 재생 또는 카피의 실행을 허용한다. 엔드-유저 장치(들)(109)는 또한 컨텐츠(113)의 최초의 카피에 있어서의 카피/재생 코드 및 임의의 새로운 2차 카피에 대한 카피/재생 코드를 적절히 갱신한다. 카피/재생 코딩은 압축된 컨텐츠(113)상에서 수행된다. 즉, 컨텐츠(113)를 압축해제해서 카피/재생 코드를 삽입(embed)할 필요가 없다.

엔드-유저 장치(들)(109)는 라이센스 워터마크(527)를 이용해서 카피/재생 모드를 컨텐츠(113)내에 삽입

한다. 삽입 알고리즘 및 연관된 스크램블링 키를 알고있는 엔드-유저 재생기 애플리케이션(195)만이 삽입된 데이터를 판독 또는 수정할 수 있다. 이 데이터는 인간 관찰자에게는 비가시 또는 비가청이며, 즉, 데이터는 컨텐츠(113)에 대해 전혀 인지가능한 손상을 주지 않는다. 워터마크는 몇 단계의 컨텐츠 처리, 즉, 데이터 압축, D-A 및 A-D 변환, 정규 컨텐츠 조작에 의해 도입되는 신호 저하를 견디므로, 워터마크는 아날로그 표현을 포함하는 임의의 표시 형태로 컨텐츠(113)와 함께 존재한다. 다른 실시예에서, 컨텐츠(113)내에 카피/재생 코드를 삽입하기 위해 라이센스 워터마크(527)를 사용하는 대신에, 엔드-유저 재생기 애플리케이션(195)은 안전하게 저장된 사용 조건(519)를 이용한다.

3. 컨텐츠 식별층(503)

컨텐츠 식별층(503) 부분으로서 컨텐츠 제공자(들)(101)는 또한 라이센스 워터마크(527)를 이용해서 컨텐츠(113)내의, 예컨대, 컨텐츠 식별자, 컨텐츠 소유자 및 다른 정보에 대해 공개일 및 지리적 배포 영역과 같은 데이터를 삽입한다. 이러한 워터마크는 여기서 저작권 워터마크(529)로서 칭한다. 수신시, 엔드-유저 장치(들)(109)는 컨텐츠(113)의 카피를 컨텐츠 구매자 이름 및 트랜잭션 ID(535)(라이센스 제어층(501) 섹션 참조)와, 라이센스 및 사용 조건(517)의 날짜와 같은 다른 정보로 워터마킹한다. 이러한 워터마크는 여기서 라이센스 워터마크로 칭한다. 인증 또는 비인증된 방법으로 획득되어 컨텐츠 품질을 보존하는 오디오 처리되는 컨텐츠(113)의 임의의 카피는 저작권 및 라이센스 워터마크를 수반한다. 컨텐츠 식별층(503)은 프라이버시를 방해한다.

4. 라이센스 제어층(501)

라이센스 제어층(501)은 비인증된 도청에 대해 컨텐츠(113)를 보호하며, 컨텐츠가 정당히 허가된 엔드-유저 장치(들)(109)를 갖는 엔드-유저(들)에 대해서만 개별적으로 해제되도록 보장하고, 인증된 전자 디지털 컨텐츠 상점(들)(103)과 라이센스 구매 트랜잭션을 성공적으로 완료한다. 라이센스 제어층(501)은 이중 암호화(531)에 의해 컨텐츠(113)를 보호한다. 컨텐츠(113)는 컨텐츠 제공자(들)(101)에 의해 발생된 암호화 대칭 키를 사용하여 암호화되며, 대칭 키는 결제소(들)의 공용 키(621)를 이용하여 암호화된다. 단지 결제소(들)(105)는 초기에 대칭 키를 복구할 수 있다.

라이센스 제어는 결제소(들)(105)에 의해 구성된 부분으로서 설계된다. 라이센스 요청(537)에 대한 허가를 해제하기 전에, (즉, 엔드-유저 장치(들)(109)에 대한 컨텐츠(113)용 대칭 키(623)), 결제소(들)(105)는 트랜잭션(541) 및 라이센스 인증(543)이 완전하고 진정함을 검증하고, 전자 디지털 컨텐츠 상점(들)(103)은 전자 컨텐츠(113) 판매에 대해 안전한 디지털 컨텐츠 전자 배포 시스템(100)으로부터의 인증을 가짐을 검증하며, 엔즈-유저(들)이 정당히 허가된 애플리케이션을 가짐을 검증한다. 회계감사/보고(545)는 보고서의 발생 및, 안전한 전자 디지털 컨텐츠 배포 시스템(100)의 다른 인증된 부분들과 라이센싱 트랜잭션 정보의 공유를 허용한다.

라이센스 제어는 SC 처리(533)를 통해 구현된다. SC(들)은 시스템 동작 구성요소들간에 암호화된 컨텐츠(113) 및 정보를 배포하는데 사용된다(SC에 대한 더욱 자세한 것을 이하의 SC(들) 세부 구조 섹션 참조). SC는 암호표기식 암호화, 디지털 서명 및 디지털 서티피케이트를 이용해서 비인증된 도청 및 전자 정보 또는 컨텐츠(113)의 수정에 대한 보호를 제공하는 암호표기식 정보 캐리어이다. 또한, 전자 데이터의 진정성 검증을 허용한다.

라이센스 제어는, 컨텐츠 제공자(들)(101), 전자 디지털 컨텐츠 상점(들)(103), 및 결제소(들)(105)가 그들을 인증하는데 사용되는 표준 서티피케이트 인증들로부터의 진정한 암호표기식 디지털 인증서를 가질것을 요구한다. 엔드-유저(들)(109)는 디지터 인증서를 가질것이 요구되지 않는다.

C. 컨텐츠 배포 및 라이센싱 제어

도 6에는 도 5에 도시된 라이센스 제어층에 적용되는 컨텐츠 배포 및 라이센싱 제어의 개관을 예시하는 블럭도가 도시되어 있다. 이 도면은 전자 디지털 컨텐츠 상점(들)103), 엔드-유저 장치(들)(109) 및 결제소(들)(105)가 인터넷을 통해 상호접속되고, 이들 구성요소간에 유니캐스트(점 대 점) 전송이 이용된 경우를 도시한다. 컨텐츠 제공자(들)(101)와 전자 디지털 컨텐츠 상점(들)(103)간의 통신은 또한 인터넷 또는 다른 네트워크를 통해 이루어질 수 있다. 컨텐츠-구매 상거래는 표준 인터넷 웹 프로토콜을 기반으로 한다고 가정한다. 웹 기반의 상호작용 부분으로서, 엔드-유저(들)는 구매할 컨텐츠(113)를 선택하고, 개인 및 금융 정보를 제공하며, 구매 조건에 동의한다. 전자 디지털 컨텐츠 상점(들)(103)은 SET와 같은 프로토콜을 이용해서 획득자 협회로부터의 지불 인증을 획득할 수 있다.

또한, 도 6에서 전자 디지털 컨텐츠 상점(들)(103)은 엔드-유저 재생기 애플리케이션(195)을 표준 웹 프로토콜에 기초한 엔드-유저 장치(들)(109)에게 다운로드하였다고 가정한다. 아키텍쳐는 전자 디지털 컨텐츠 상점(들)(103)이 다운로드된 재생기 애플리케이션(195)에 대해 고유 애플리케이션 ID를 할당하고, 엔드-유저 장치(들)(109)이 차후의 애플리케이션 라이센스 검증(이후 설명될)을 위해 그것을 저장할 것을 요구한다.

전체적인 라이센싱 흐름은 컨텐츠 제공자(들)(101)에서 시작한다. 컨텐츠 제공자(들)(101)는 국부적으로 발생된 암호화 대칭 키를 이용해서 컨텐츠(113)를 암호화하며, 결제소(들)(105) 공용 키(621)를 이용해서 대칭 키(623)를 암호화한다. 다른 실시예에서, 대칭 키는 국부적으로 발생되는 대신에 결제소(들)(105)로부터 컨텐츠 제공자(들)(101)에게로 송신될 수 있다. 컨텐츠 제공자(들)(101)는 암호화된 컨텐츠(113) 주위의 컨텐츠 SC(들)(630), 암호화된 대칭 키(623) 주위의 메타데이터 SC(들)(620) 및 다른 컨텐츠(113) 관련 정보를 생성한다. 모든 컨텐츠(113) 객체에 대해 하나의 메타데이터 SC(들)(620)와 하나의 컨텐츠 SC(들)(630)이 존재한다. 컨텐츠(113) 객체는 압축 레벨 하나의 동일 노래일 수 있고 또는 컨텐츠(113) 객체는 앨범상의 각 노래일 수 있고 또는 컨텐츠(113) 객체에 대해, 메타데이터 SC(들)(620)는 또한 컨텐츠 사용 제어층(505)과 연관된 상점 사용 조건(519)를 갖는다.

컨텐츠 제공자(들)(101)는 메타데이터 SC(들)(620)를 하나 이상의 전자 디지털 컨텐츠 상점(들)(103)에게 배포(단계 601)하고, 컨텐츠 SC(들)(630)를 하나 이상의 컨텐츠 호스팅 사이트에게 배포(단계 602)한다.

각각의 전자 디지털 컨텐츠 상점(들)(103)은, 순서대로 제의 SC(들)(641)를 생성한다. 제의 SC(들)(641)는 전형적으로 메타데이터 SC(들)(620)로서 컨텐츠 제공자(들)(101)의 디지털 서명(624) 및 컨텐츠 제공자(들)(101)의 인증서(도시되지 않음)를 포함하는 동일 정보의 많은 량을 포함한다. 앞서 언급된 바와 같이, 전자 디지털 컨텐츠 상점(들)(103)은 초기에 컨텐츠 제공자(들)(101)에 의해 정의된 상점 사용 조건(519)(제어 사용 제어층에 의해 처리됨)을 늘리거나 줄일 수 있다. 선택사양적으로, 컨텐츠 SC(들)(630) 및/또는 메타데이터 SC(들)(620)은 컨텐츠 제공자(들)(101)의 디지털 서명(624)으로 서명된다.

엔드-유저 장치(들)(109)와 전자 디지털 컨텐츠 상점(들)(103)간의 컨텐츠-구매 트랜잭션의 완료(단계 603) 후에, 전자 디지털 컨텐츠 상점(들)(103)은 트랜잭션 SC(들)(640)을 생성해서 엔드-유저 장치(들)(109)에게로 전송(단계 604)한다. 트랜잭션 SC(들)(640)는 고유 트랜잭션 ID(535), 구매자의 이름(즉, 엔드-유저(들)의 이름)(도시되지 않음), 엔드-유저 장치(들)(109)의 공용 키(661) 및 구매한 컨텐츠(113)와 연관된 제의 SC(들)(641)을 포함한다. 도 6에 도시된 트랜잭션 데이터(642)는 트랜잭션 ID(535)와 엔드-유저(들) 이름(도시되지 않음)을 나타낸다. 트랜잭션 데이터(642)는 결제소(들)(105)의 공용 키(621)로 암호화된다. 선택사양적으로, 트랜잭션 SC(들)(640)는 JS자 디지털 컨텐츠 상점(들)(103)의 디지털 서명(643)으로 서명된다.

트랜잭션 SC(들)(640)(및 그에 포함된 제의 SC(들)(641))의 수신시, 엔드-유저 장치(들)(109)상에서 실행중인 엔드-유저 재생기 애플리케이션(195)은 주문 SC(들)(650)에 의해 결제소(들)(105)로부터 라이센스 인증을 구한다(단계 605). 주문 SC(들)(650)는 제의 SC(들)(641)로부터 암호화된 대칭 키(623) 및 상점 사용 조건(519)와, 트랜잭션 SC(들)(640)로부터 암호화된 트랜잭션 데이터(642)와, 엔드-유저 장치(들)(109)로부터 암호화된 애플리케이션 ID(551)를 포함한다. 다른 실시예에서, 주문 SC(들)(650)는 엔드-유저 장치(들)(109)의 디지털 서명(652)으로 서명된다.

엔드-유저 장치(들)(109)로부터 주문 SC(들)(650) 수신시, 결제소(들)(105)는

1. 전자 디지털 컨텐츠 상점(들)(103)이 안전한 디지털 컨텐츠 전자 배포 시스템(100)(결제소(들)(105)의 데이터베이스(160)에 존재함)로부터의 인증을 갖고,

2. 주문 SC(들)(650)가 변경되지 않았으며,

3. 트랜잭션 데이터(642) 및 대칭 키(623)가 완전하고 진정하고,

4. 엔드-유저 장치(들)(109)에 의해 구매된 전자 상점 사용 조건(519)이 컨텐츠 제공자(들)(101)에 의해 설정된 그들 사용 조건(517)과 일치하며,

5. 애플리케이션 ID(551)가 유효 구조를 갖고 그것이 인증된 전자 디지털 컨텐츠 상점(들)(103)에 의해 제공된 것임

을 검증한다.

검증이 성공하면, 결제소(들)(105)는 대칭 키(623)와 트랜잭션 데이터(642)를 암호해독해서 라이센스 SC(들)(660)를 구축해서 엔드-유저 장치(들)(109)에게로 전송한다(단계 606). 라이센스 SC(들)(660)는 대칭 키 (623) 및 트랜잭션 데이터(642)를 포함하며, 이들은 엔드-유저 장치(들)(109)의 공용 키(661)를 이용해서 암호화된다. 어느 것이라도 검증이 실패하면, 결제소(들)(105)는 엔드-유저 장치(들)(109)에 대한 라이센스를 거절하고 엔드-유저 장치(들)(109)에게 통지한다. 결제소(들)(105)는 또한 이러한 검증 실패를 전자 디지털 컨텐츠 상점(들)(103)에게 즉시 통지한다. 다른 실시예에서, 결제소(들)(105)는 라이센스 SC(들)(660)를 그의 디지털 서명(663)으로 서명한다.

라이센스 SC(들)(660)를 수신한 후, 엔드-유저 장치(들)(109)는 결제소(들)(105)로부터 앞서 수신된 대칭 키(623) 및 트랜잭션 데이터(642)를 암호해독하며, 컨텐츠 호스팅 사이트(들)(111)로부터 컨텐츠 SC(들)(630)를 요구한다(단계 607). 컨텐츠 SC(들)(630)의 도달시, 엔드-유저 장치(들)(109)는 대칭 키(623)를 이용해서 컨텐츠(113)를 암호해독하며, 컨텐츠(113) 및 트랜잭션 데이터(642)를 라이센스 워터마킹, 카피/재생 코딩, 스크램블링 및 도 5에 이미 기술된 바와 같은 다른 컨텐츠(113) 처리를 위해 다른 유틸에게로 전송한다.

마지막으로, 결제소(들)(105)는 주기적으로 회계감사 및 트래킹을 목적으로 요약 트랜잭션 보고를 컨텐츠 제공자(들)(101) 및 전자 디지털 컨텐츠 상점(들)(103)에게로 전송한다(단계 610).

V. 안전한 컨테이너 구조

A. 전반적 구조

안전한 컨테이너(SC)는, 함께 컨텐츠(113)의 단위 또는 트랜잭션의 일부를 정의하고 또한 사용 조건, 메타데이터 및 암호화 방법들과 같은 관련 정보를 정의하는 몇개의 부분들로 구성되는 구조이다. SC(들)는 정보의 보전성, 완전성 및 진실성이 검증될 수 있는 방법으로 설계된다. SC(들)의 정보중 몇몇은 적절한 인증이 획득된 후에만 액세스될 수 있도록 암호화될 수 있다.

SC(들)는 SC(들) 및 그에 포함된 각 부분들에 대한 정보를 기록하는 적어도 하나의 빌 자료(BOM)를 포함한다. 메시지 다이제스트가 MD-5와 같은 해싱 알고리즘을 이용해서 각 부분에 대해 계산된 후, 그 부분에 대한 BOM 레코드에 포함된다. 부분들의 다이제스트는 함께 연쇄되고, 다른 다이제스트는 그들로부터 계산된 후, SC(들)를 생성하는 엔티티의 개인 키를 이용해서 암호화되어 디지털 서명을 생성한다. SC(들)를 수신하는 부분들은 디지털 서명을 이용해서 모든 다이제스트를 검증할 수 있고, 따라서, SC(들) 및 그의 모든 부분들에 대한 보전성 및 완전성을 유효화시킬 수 있다.

다음의 정보가 각 부분에 대해 레코드와 함께 BOM의 레코드로서 포함될 수 있다. SC(들) 유형은 어느 레코드가 포함되어야 할지를 결정한다.

· SC(들) 버전

· SC(들) ID

· SC(들)의 유형(예컨대, 제의, 주문, 트랜잭션, 컨텐츠, 메타데이터 또는 판촉 및 라이센스)

· SC(들)의 공개자

· SC(들)를 생성한 데이터

· SC(들)의 만료일

· 결제소(들) URL

· 포함된 부분에 대해 사용된 다이제스트 알고리즘의 설명(디폴트는 MD-5)

· 디지털 서명 암호화에 사용된 알고리즘의 설명(디폴트는 RSA)

· 디지털 서명(포함된 부분들의 모든 연쇄된 다이제스트들의 암호화된 다이제스트)

SC(들)는 둘 이상의 BOM을 포함할 수 있다. 예컨대, 제의 SC(들)(641)는 전자 디지털 컨텐츠 상점(들)(103)에 의해 부가된 부가 정보 및 새로운 BOM은 물론, 부분들의 BOM을 포함하는 최초의 메타데이터 SC(들)(620) 부분들로 구성된다. 메타데이터 SC(들)(620) BOM에 대한 레코드는 제의 SC(들)(641) BOM에 포함된다. 이 레코드는 그의 보전성을 유효화하는데 사용될 수 있는 메타데이터 SC(들)(620) BOM에 대한 다이제스트를 포함하며, 따라서, 메타데이터 SC(들)(620)으로부터 포함된 부분들의 보전성은 또한 메타데이터 SC(들)(620) BOM에 저장된 부분 다이제스트 값을 이용해서 유효화될 수 있다. 메타데이터 SC(들)(620)로부터의 부분들중 어느것도 제의 SC(들)(641)에 대해 생성되었던 새로운 BOM의 레코드를 갖지 않는다. 전자 디지털 컨텐츠 상점(들)(103) 및 메타데이터 SC(들)(620) BOM에 의해 부가된 부분들만이 새로운 BOM의 레코드를 갖는다.

SC(들)는 또한 키 설명 부분을 포함할 수 있다. 키 설명 부분은 SC(들)의 암호화된 부분들에 대한 다음 정보를 갖는 레코드를 포함한다.

· 암호화된 부분의 이름

· 암호해독될 때 그 부분에 대해 사용할 이름

· 부분을 암호화하는데 사용된 암호화 알고리즘

· 부분을 암호화하는데 사용되었던 공용 암호화 키를 표시하기 위한 키 식별자 또는 암호호해독될 때 암호화된 부분을 암호해독하는데 사용되는 암호화된 대칭키

· 대칭 키를 암호화하는데 사용된 암호화 알고리즘. 이 영역은 키 설명 부분이 암호화된 부분을 암호화하는데 사용되었던 암호화된 대칭 키를 포함하는 경우에만 제공된다.

· 대칭 키를 암호화하는데 사용되었던 공용 암호화 키의 키 식별자. 이 영역은 키 설명 부분의 레코드가 암호화된 대칭 키 및 암호화된 부분을 암호화하는데 사용하였던 대칭 키의 암호화 알고리즘 식별자를 포함하는 경우에만 제공된다.

SC(들)이 암호화된 부분을 전혀 포함하지 않는 경우, 키 설명 부분을 존재하지 않는다.

B. 권리 관리 언어 구문론 및 의미론

권리 관리 언어는 컨텐츠(113) 구매후 엔드-유저(들)에 의한 컨텐츠(113) 사용에 대해 제약을 정의하기 위해 할당된 값일 수 있는 파라미터들로 구성된다. 컨텐츠(113) 사용에 대한 제약은 사용 조건(517)이다. 각각의 컨텐츠 제공자(들)(101)는 그의 각 컨텐츠(113) 항목에 대해 사용 조건(517)을 지정한다. 전자 디지털 컨텐츠 상점(들)(103)은 메타데이터 SC(들)(620)에 사용 조건(517)을 기술하며, 이 정보를 사용해서 컨텐츠(113)에 대한 소매 구매 정보를 부가하는 것은 물론 그들의 고객에게 제의하기를 원하는 선택사양들을 제공한다. 엔드-유저(들)가 구매를 위해 컨텐츠(113) 항목을 선택한 후, 엔드-유저 장치(들)(109)는 상점 사용 조건(519)에 근거해 컨텐츠(113)에 대한 인증을 요구한다. 결제소(들)(105)가 엔드-유저(들)에게로 라이센스 SC(들)(660)를 송신하기 전에, 결제소(들)(105)는 요구중인 상점 사용 조건(519)이 메타데이터 SC(들)(620)내에 컨텐츠 제공자(들)(101)에 의해 지정된 허용가능한 사용 조건들(517)과 일치하는지를 검증한다.

엔드-유저 장치(들)(109)가 구매된 컨텐츠(113)를 수신할 때, 상점 사용 조건(519)은 워터마킹 툴을 이용해서 그 컨텐츠(113)내로 암호화되거나 안전하게 저장된 사용 조건(519)에 암호화된다. 엔드-유저 장치(들)(109)상에서 실행중인 엔드-유저 재생기 애플리케이션(195)은 컨텐츠(113)내로 암호화된 상점 사용 조건(519)이 적용될 것을 보장한다.

다음은 컨텐츠(113)가 음악인 경우의 실시예에 대한 상점 사용 조건(519)의 예이다.

· 노래가 녹음가능하다.

· 노래가 n회 재생될 수 있다.

C. 안전한 컨테이너 흐름 및 처리의 개관

메타데이터 SC(들)(620)는 컨텐츠 제공자(들)(101)에 의해 구축되며, 노래들과 같은 컨텐츠(113) 항목들을 정의하는데 사용된다. 컨텐츠(113) 자체는, 그 사이즈가 통상 전자 디지털 컨텐츠 상점(들)(103) 및 엔드-유저(들)에게는 너무 커서 단지 설명적 메타데이터를 액세스할 목적으로 컨테이너를 효율적으로 다운로드할 수 없기 때문에 이들 SC(들)에 포함되지 않는다. 대신에, SC(들)는 컨텐츠(113)를 가리키도록 URL(Uniform Resource Locators)을 포함한다. 또한, SC(들)는 컨텐츠(113)에 대한 기술 정보 및, 노래 컨텐츠(113)의 경우에서 음악, CD 커버 기술 및/또는 디지털 오디오 클립에 대한 것과 같은 임의의 다른

연관 데이터를 제공하는 메타데이터를 포함한다.

전자 디지털 컨텐츠 상점(들)(103)은 그들이 인증받은 메타데이터 SC(들)(620)를 다운로드하고 제의 SC(들)(641)를 구축한다. 요약하면, 제의 SC(들)(641)는 전자 디지털 컨텐츠 상점(들)(113)에 의해 포함된 부가 정보와 합께 메타데이터 SC(들)(620)로부터의 BOM과 몇몇 부분들로 구성된다. 제의 SC(들)(641)에 대한 새로운 BOM은 제의 SC(들)(641)가 구축될 때 생성된다. 전자 디지털 컨텐츠 상점(들)(103)은 또한 그들로부터 메타데이터 정보를 추출해서 그들의 웹 사이트상에 통상 엔드-유저(들)가 컨텐츠(113)를 구매할 수 있도록 엔드-유저(들)에게 컨텐츠(113)의 설명을 제공하는 HTML 페이지를 구축함으로써 메타데이터 SC(들)(620)를 사용한다.

전자 디지털 컨텐츠 상점(들)(103)에 의해 부가된 제의 SC(들)(641)내의 정보는 통상 메타데이터 SC(들)(620)에 지정된 사용 조건(517)의 선택 및, 상점 로고의 그래픽 이미지 화일 및 상점의 웹 사이트에 대한 URL과 같은 판촉 데이터를 한정하는 것이다. 메타데이터 SC(들)(620)에서 제의 SC(들)(641) 템플레이트는, 제의 SC(들)(641)에서 어느 정보가 전자 디지털 컨텐츠 상점(들)(103)에 의해 무효화될 수 있는지, 있다면 어떤 부가의 데이터가 전자 디지털 컨텐츠 상점(들)(103)에 의해 요구되는지 및 매립된 메타데이터 SC(들)(620)내에 어떤 부분이 유지되는지를 표시한다.

제의 SC(들)(641)는, 엔드-유저(들)가 전자 디지털 컨텐츠 상점(들)(103)으로부터 컨텐츠(113)를 구매하기로 결정했을 때 트랜잭션 SC(들)(640)에 포함된다. 전자 디지털 컨텐츠 상점(들)(103)은 트랜잭션 SC(들)(640)를 구축하며, 구매되는 각각의 컨텐츠(113) 항목에 대해 제의 SC(들)(641)을 포함시키며, 그것을 엔드-유저 장치(들)(109)에게로 전송한다. 엔드-유저 장치(들)(109)는 트랜잭션 SC(들)(640)를 수신하며, 트랜잭션 SC(들)(640) 및 포함된 제의 SC(들)(641)의 보전성을 유효화시킨다.

주문 SC(들)(650)는 구매되는 각각의 컨텐츠(113) 항목에 대해 엔드-유저 장치(들)(109)에 의해 구축된다. 제의 SC(들)(641)로부터, 트랜잭션 SC(들)(640)로부터 및 엔드-유저 장치(들)(109)의 구성 화일들로부터의 정보가 포함된다. 주문 SC(들)(650)는 한번에 하나씩 결제소(들)(105)에게로 전송된다. 결제소(들)(105) URL., 이 경우 주문 SC(들)(650)는 메타데이터 SC(들)(620)에 대한 BOM내의 레코드들중 하나로서 포함되며, 제의 SC(들)(641)에 또한 포함된다.

결제소(들)(105)는 주문 SC(들)(650)를 유효화시켜 처리해서 엔드-유저 장치(들)(109)에게 라이센스 워터마크(527) 및 구매된 컨텐츠(113)를 엑세스하는데 요구된 모든것을 제공한다. 결제소(들)(105)의 기능들중 하나는 제의 SC(들)(641)로부터의 워터마킹 인스트럭션 및 컨텐츠 SC(들)(630)로부터의 컨텐츠(113)를 암호해독하는데 필요한 대칭 키(623)를 암호해독하는 것이다. 암호화된 대칭 키(623) 레코드는 사실상 실제의 암호화된 대칭 키(623) 이상을 포함한다. 암호화를 실행하기 전에, 컨텐츠 제공자(들)(101)는 선택사양적으로 자신의 이름을 실제의 대칭 키(623)에 첨부할 수 있다. 컨텐츠 제공자(들)(101) 이름이 대칭 키(623)와 합께 암호화된 경우, 리갈 SC(들)로부터 자신의 메타데이터 SC(들)(620) 및 컨텐츠 SC(들)(630)를 구축한 개인 컨텐츠 제공자(들)(101)에 대한 보안성이 제공된다. 결제소(들)(105)는 대칭 키(623)와 합께 암호화된 컨텐츠 제공자(들)(101)의 이름이 SC(들) 인증서내의 컨텐츠 제공자(들)(101) 이름과 일치하는지를 검증한다.

결제소(들)(105)에 의한 워터마킹 인스트럭션에 대해 행해지도록 요구된 어떤 변화가 있는 경우, 결제소(들)(105)는 대칭 키(623)를 암호해독한 후, 워터마킹 인스트럭션을 수정하고 새로운 키(623)를 사용해서 그들을 다시 암호화한다. 그리고 나서, 대칭 키(623)는 엔드-유저 장치(들)(109)의 공용 키(661)를 이용해서 재암호화된다. 결제소(들)(105)는 또한 SC(들)내의 다른 대칭 키(623)를 암호해독하며, 그들을 엔드-유저 장치(들)(109)의 공용 키(661)로 다시 암호화한다. 결제소(들)(105)는 새로이 암호화된 대칭 키(623)와 갱신된 워터마킹 인스트럭션을 포함하는 라이센스 SC(들)(660)를 구축해서 그것을 주문 SC(들)(650)에 응답해서 엔드-유저 장치(들)(109)에게로 전송한다. 주문 SC(들)(650)의 처리가 성공적으로 완료되지 않으면, 결제소(들)(105)는 엔드-유저 장치(들)(109)에게로 인용 프로세스의 실패를 보고하는 HTML 페이지 또는 그의 등가물을 복귀시킨다.

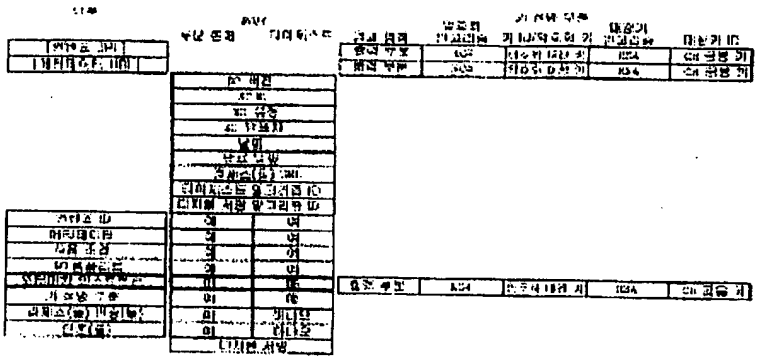
라이센스 SC(들)(660)는 엔드-유저 장치(들)(109)에게 컨텐츠(113) 항목을 엑세스하는데 필요한 모든 것을 제공한다. 엔드-유저 장치(들)(109)는 컨텐츠 호스팅 사이트(들)(111)로부터 적절한 컨텐츠 SC(들)(630)를 요구한다. 컨텐츠 SC(들)(630)는 컨텐츠 제공자(들)(101)에 의해 구축되며, 암호화된 컨텐츠(113) 및 메타데이터 부분을 포함한다. 엔드-유저 재생기 애플리케이션(195)은 라이센스 SC(들)(660)로부터의 대칭 키(623)를 이용해서 컨텐츠(113), 메타데이터 및 워터마킹 인스트럭션을 암호해독한다. 그리고 나서, 워터마킹 인스트럭션은 컨텐츠(113)내로 첨부되며, 컨텐츠(113)는 스크램블되어 엔드-유저 장치(들)(109)상에 저장된다.

0. 메타데이터 안전한 컨테이너 620 포맷

다음의 표는 메타데이터 SC(s) 620에 포함되는 부분을 나타낸다. 부분 칼럼의 각각의 박스는 BOM([] 문자에 의해 둘러싸인 부분의 명칭을 제외함)과 합께 SC(s)에 포함된 개별적인 객체이다. BOM은 SC(s)에 포함된 각각의 부분에 대한 레코드(record)를 포함한다. 부분 존재 칼럼은 부분 자체가 실질적으로 SC(s)에 포함되는지 여부를 나타내고, 다이제스트 칼럼은 부분에 대해 메시지 다이제스트가 연산되는지 여부를 나타낸다. 최초의 전체 BOM이 전파된다 하더라도, SC(s)가 (연관된 템플릿에 의해 결정되는) 다른 SC(s)에 포함되는 경우 몇몇 부분은 전파되지 않을 수도 있다. 이와 같이 행해지는 이유는 전체 BOM이 최초의 SC(s)내의 디지털 서명을 확인하도록 결제소(들)(105)에 의해 요구되기 때문이다.

다음 표의 키 설명 부분 칼럼은 SC(s)의 키 설명 부분에 포함되는 레코드를 정의한다. 키 설명 부분의 레코드는 SC(s)내의 부분 또는 다른 SC(s)내의 부분을 암호화하도록 사용된 암호화 키 및 알고리즘에 관한 정보를 정의한다. 각각의 레코드는 암호화된 부분 명칭을 포함하고, 필요하다면, 암호화된 부분을 포함하는 다른 SC(s)를 지정하는 URL을 포함한다. 결과 명칭 칼럼은 복호화된 후, 부분에 할당되는 명칭을 정의한다. 암호화 알고리즘 칼럼은 부분을 암호화하기 위해 사용된 암호화 알고리즘을 정의한다. 키 Id/암호화 키 칼럼은 부분을 암호화하기 위해 사용된 암호화키의 식별부 또는 부분을 암호화하기 위해 사용된 암호화된 대칭 키(623) 비트 스트링의 베이스 64 암호화를 정의한다. 대칭 키 알고리즘 칼럼은 대응의 칼럼이 암호화된 대칭 키(623)인 경우 대칭 키(623)를 암호화하도록 사용된 암호화 알고리즘을 정의

하는 선택사양적인 파라미터이다. 대칭 키 ID 칼럼은 키 Id/암호화 키 칼럼이 대칭 키(623)로 암호화되는 경우 대칭 키(623)를 암호화하도록 사용된 암호화키의 식별부이다.



다음은 상기 메타데이터 SC(s) 표에서 사용되는 용어를 설명한다.

· [컨텐츠 URL] - 키 설명 부분의 레코드의 파라미터. 이것은 이러한 메타데이터 SC(s)(620)와 연관되는 컨텐츠 SC(s)(630)내의 암호화된 컨텐츠(113)를 지정하는 URL이다. 메타데이터 SC(s)(620) 자체는 암호화된 컨텐츠(113)를 포함하지 않는다.

· [메타데이터 URL] - 키 설명 부분의 레코드의 파라미터. 이것은 이러한 메타데이터 SC(s)(620)와 연관되는 컨텐츠 SC(s)(630)내의 암호화된 메타데이터를 지정하는 URL이다. 메타데이터 SC(s)(620) 자체는 암호화된 메타데이터를 포함하지 않는다.

· 컨텐츠 ID - 컨텐츠(113) 항목에 할당된 고유의 ID를 정의하는 부분. 메타데이터 SC(s)(620)가 둘 이상의 컨텐츠(113) 항목을 참조하는 경우 이러한 부분에 포함된 둘 이상의 컨텐츠 ID가 존재한다.

· 메타데이터 - 노래의 경우 아티스트 명칭 및 CD 커버 분야와 같은 컨텐츠(113) 항목과 관련된 정보를 포함하는 부분. 다수의 메타데이터 부분이 존재할 수 있으며, 이들 중 일부는 암호화될 수도 있다. 메타데이터 부분의 내부 구조는 내부에 포함된 메타데이터의 유형에 따라 달라진다.

· 사용 조건 - 컨텐츠(113)의 사용을 위한 엔드 유저(들)상에 부과될 사용 옵션, 규칙, 제한을 설명하는 정보를 포함하는 부분.

· SC(s) 템플리트 - 제의, 주문, 라이센스 SC(s)(660)를 구축하는 요구된 정보 및 선택사양적인 정보를 설명하는 템플리트를 정의하는 부분.

· 워터마킹 인스트럭션 - 컨텐츠(113)내에 워터마킹을 구현하는 암호화된 인스트럭션 및 파라미터를 포함하는 부분. 워터마킹 인스트럭션은 결제소(들)(105)에 의해 수정될 수 있으며, 라이센스 SC(s)(660)내의 엔드 유저 디바이스(들)(109)로 반환될 수도 있다. 워터마킹 인스트럭션을 암호화하는데 사용된 암호화 알고리즘, 워터마킹 인스트럭션이 암호화되는 경우에 사용할 출력 부분 명칭, 워터마킹 인스트럭션을 암호화하는데 사용된 암호화된 대칭 키(623) 비트 스트링의 베이스 64 암호화, 대칭 키(623)를 암호화하는데 사용된 암호화 알고리즘, 대칭 키(623)를 암호화하는데 요구되는 공용키의 식별부를 정의하는 키 설명 부분에 레코드가 존재한다.

· 결제소(들) 인증(들) - 인증 관청으로부터 또는 결제소(들)(105)의 서명된 공용키(621)를 포함하는 결제소(들)(105)로부터의 인증서. 둘 이상의 인증서가 존재할 수도 있으며, 이 경우 계층적 레벨 구조는 결제소(들)(105)의 공용키(621)를 포함하는 최저 레벨 인증서가 도달할 때까지 다음의 최저 레벨 인증서를 개방할 공용키를 포함하는 최고 레벨 인증서와 함께 사용된다.

· 인증서(들) - 인증 관청으로부터 또는 SC(s)를 생성한 엔티티의 서명된 공용키(621)를 포함하는 결제소(들)(105)로부터의 인증서. 둘 이상의 인증서가 존재할 수도 있으며, 이 경우 계층적 레벨 구조는 SC(s) 생성자의 공용키를 포함하는 최저 레벨 인증서가 도달될 때까지 다음 레벨 인증서 등을 개방할 공용키를 포함하는 최고 레벨 인증서와 함께 사용된다.

· SC 버전 - SC 패커 툴(Packer Tool)에 의해 SC(s)에 할당된 버전 번호.

· SC ID - SC(s)를 생성한 엔티티에 의해 SC(s)에 할당된 고유의 ID.

· SC 유형 - SC(s)의 유형(예를 들어, 메타데이터, 제의, 주문, 등)을 표시함.

· SC 발표자 - SC(s)를 생성한 엔티티를 표시함.

· 생성 날짜 - SC(s)가 생성된 날짜.

· 만료 날짜 - SC(s)가 만료하여 더 이상 유효하지 않은 날짜.

· 결제소(들) URL - 엔드 유저 플레이어 애플리케이션(195)이 컨텐츠(113)를 액세스할 적절한 허가를 획득하기 위해 상호 작용하는 결제소(들)(105)의 어드레스.

· 다이제스트 알고리즘 ID - 부분의 다이제스트를 연산하는데 사용된 알고리즘의 식별자

디지털 서명 알고리즘 ID - 연결 부분 다이제스트의 다이제스트를 암호화하는데 사용된 알고리즘의 식별자. 이 암호화된 값은 디지털 서명이다.

· 디지털 서명 - SC(s)를 생성한 엔티티의 공용키와 함께 암호화된 연결 부분 다이제스트의 다이제스트.

· 출력 부분 - 암호화된 부분이 복호화되는 경우 출력 부분을 할당하는 명칭.

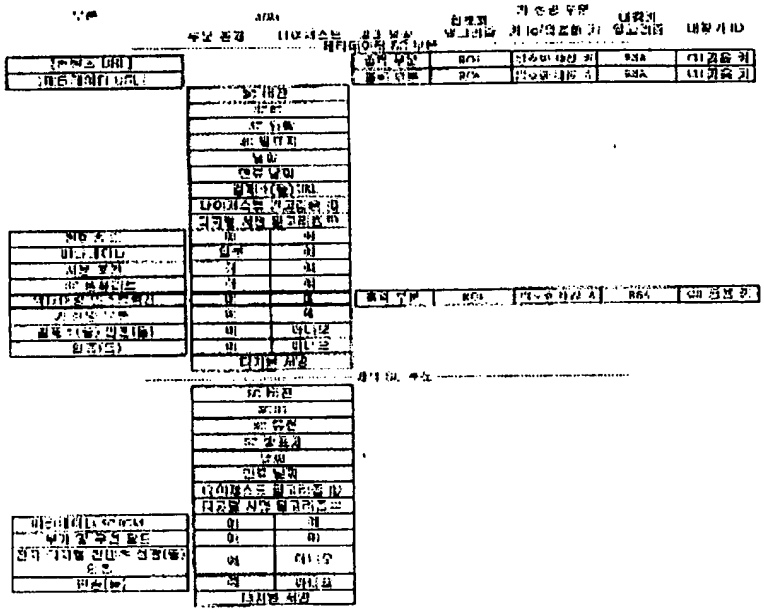
· RSA 및 RC4 - 대칭 키(623) 및 데이터 부분을 암호화하는데 사용된 디폴트 암호화 알고리즘.

· 암호화 대칭 키 - 복호화되는 경우, SC(s) 부분을 복호화하는데 사용된 암호화된 키 비트 스트링의 베이스 64 암호화.

· CH 공용키 - 결제소(들)(105) 공용키(621)가 데이터를 암호화하는데 사용됨을 표시하는 식별자.

E. 제의 안전한 컨테이너 641 포맷

다음의 표는 제의 SC(s)(641)에 포함되는 부분을 도시한다. 메타데이터의 일부를 제외한 부분, 및 메타데이터 SC(s)(620)로부터의 BOM은 제의 SC(s)(641)에 또한 포함된다.



다음은 다른 SC(s)에 대해 이전에 설명되지 않은 상기 제의 SC(s)(641)에서 사용되는 용어를 설명한다.

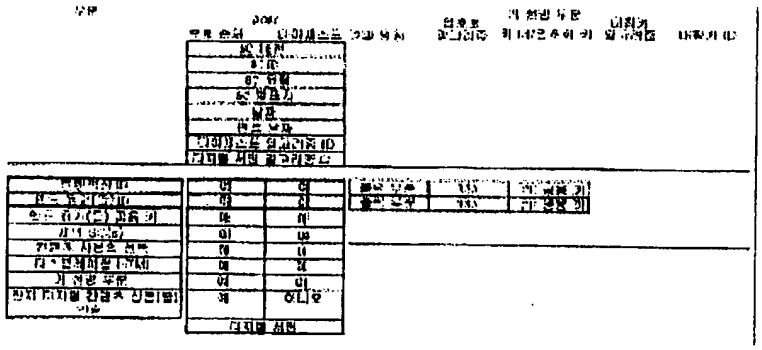
· 메타데이터 SC(s) BOM - 최초의 메타데이터 SC(s)(620)로부터의 BOM. 제의 SC(s)(641) BOM의 레코드는 메타데이터 SC(s)(620) BOM의 다이제스트를 포함한다.

· 부가 및 우선 필드 - 전자 디지털 컨텐츠 상점(들)(103)에 의해 우선되는 사용 조건 정보. 이 정보는 결제소(들)(105)에 의해 유효화되며, 수신된 SC(s) 템플릿에 의해, 전자 디지털 컨텐츠 상점(들)(103)이 우선하는 임의의 것이 그 허가 범위 내에 있음을 보장한다.

· 전자 디지털 컨텐츠 상점(들) 인증서 - 결제소(들)(105)에 의해 전자 디지털 컨텐츠 상점(들)(103)에 제공되고 그 전용키를 이용하여 결제소(들)(105)에 의해 서명된 인증서. 이 인증서는 엔드 유저 플레이어 애플리케이션(105)에 의해 사용되어 전자 디지털 컨텐츠 상점(들)(103)이 컨텐츠(113)의 유효한 배포자임을 확인한다. 엔드 유저 플레이어 애플리케이션(195) 및 결제소(들)(105)는 결제소(들)(105) 공용키(621)로 인증 서명을 복호화함으로써 허가된 배포자임을 확인할 수 있다. 엔드 유저 플레이어 애플리케이션(195)은 인스톨 동안 그 초기화의 일부로서 수신하는 결제소(들)(105) 공용키(621)의 로컬 카피를 유지한다.

F. 트랜잭션 안전한 컨테이너 640 포맷

다음의 표는 BOM 및 키 설명 부분과 함께 트랜잭션 SC(s)(640)에 포함되는 부분을 도시한다.



다음은 다른 SC(s)에 대해 이전에 설명되지 않은 상기 트랜잭션 SC(s)(640)에서 사용되는 용어를 설명한다.

· 트랜잭션 ID(535) - 트랜잭션을 고유하게 식별하는 전자 디지털 컨텐츠 상점(들)(103)에 의해 할당된 ID.

· 엔드 유저(들) ID - 엔드 유저(들)가 구매 선택하고 신용 카드 정보를 제공할 때 전자 디지털 컨텐츠 상점(들)(103)에 의해 획득된 엔드 유저(들)의 식별부.

· 엔드 유저(들)의 공용키 - 대칭 키(623)를 재암호화하는 결제소(들)(105)에 의해 사용되는 엔드 유저(들)의 공용키(661). 엔드 유저(들)의 공용키(661)는 구입 트랜잭션 동안 전자 디지털 컨텐츠 상점(들)(103)으로 전송된다.

· 제의 SC(s) - 구입된 컨텐츠(113) 항목에 대한 제의 SC(s)(641).

· 컨텐츠 사용의 선택 - 엔드 유저(들)에 의해 구입되는 각각의 컨텐츠(113) 항목에 대한 사용 조건의 어레이. 각각의 제의 SC(s)(641)에 대한 엔트리가 존재한다.

· 디스플레이할 HTML - 엔드 유저(들) 플레이어 애플리케이션(195)이 트랜잭션 SC(s)(640)의 수신시에 또는 엔드 유저 디바이스(들)(109) 및 결제소(들)(105)간의 상호 작용 동안 인터넷 브라우저 윈도우에 디스플레이하는 둘 이상의 HTML 페이지.

엔드 유저 디바이스(들)(109)가 트랜잭션 SC(s)(640)를 수신하는 경우, SC(s)의 통합성 및 허가를 확인하도록 다음의 단계가 수행될 수도 있다.

1. 결제소(들)(105)의 공용키(621)를 이용하여 전자 디지털 컨텐츠 상점(들)(103) 인증서의 통합성을 확인한다. 결제소(들)(105)의 공용키(621)는 그 인스톨 프로세스 동안 엔드 유저 플레이어 애플리케이션(195)의 초기화 일부로서 수신된 후에 엔드 유저 디바이스(들)(109)에 저장된다.

2. 전자 디지털 컨텐츠 상점(들)(103) 인증서로부터의 공용키를 이용하여 SC(s)의 디지털 서명(643)를 확인한다.

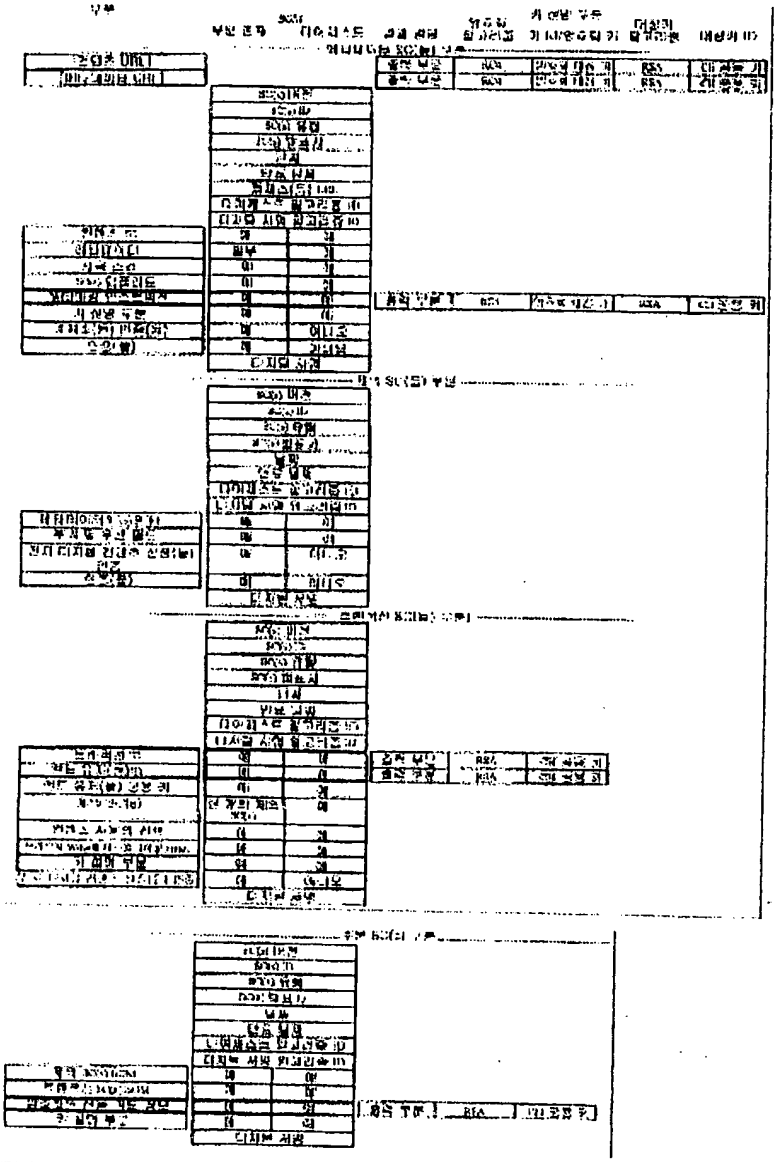
3. SC(s) 부분의 해쉬(hashes)를 확인한다.

4. 트랜잭션 SC(s)(640)에 포함된 각각의 제의 SC(s)(641)의 통합성 및 허가를 확인한다.

6. 주문 안전한 컨테이너(650) 포맷

다음의 표는 BOM 및 키 설명 부분과 함께 주문 SC(s)(650)에 포함되는 부분을 나타낸다. 이러한 부분은 복호화 및 확인을 위해 결제소(들)(105)에 정보를 제공하거나 또는 결제소(들)(105)에 의해 유효화된다. 제의 SC(s)(641)로부터의 부분 및 BOM은 주문 SC(s)(650)에 또한 포함된다. 메타데이터 SC(s) BOM의 부분 존재 랄럼의 몇몇 스트링은 이들 부분의 일부가 주문 SC(s)(650)에 포함되지 않음을 나타낸다. 메타데이터 SC(s)(620)로부터의 BOM은 임의의 변경없이 또한 포함됨에 따라 결제소(들)(105)는 메타데이터

SC(s)(620) 및 그 부분의 통합성을 유효화할 수 있다.



다음은 다른 SC(s)에 대해 이전에 설명되지 않은 상기 주문 SC(s)(650)에서 사용되는 용어를 설명한다.

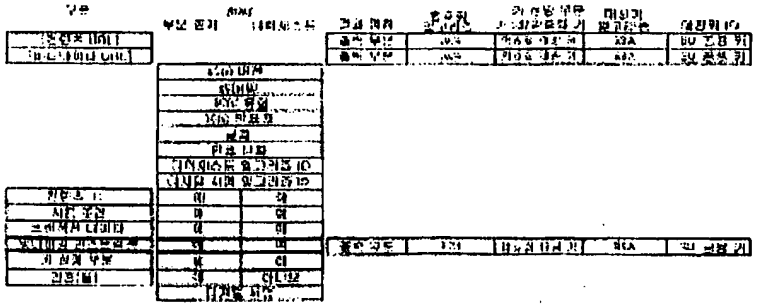
· 트랜잭션 SC(s) BOM - 최초의 트랜잭션 SC(s)(640)내의 BOM. 주문 SC(s)(650) BOM의 레코드는 트랜잭션 SC(s)(640) BOM의 다이제스트를 포함한다.

· 암호화된 신용 카드 정보 - 신용 카드 또는 청구서 카드로 구입한 것을 청구하는데 사용되는 엔드 유저(들)로부터의 선택사양적인 암호화된 정보. 이 정보는 제의 SC(s)(641)를 생성한 전자 디지털 컨텐츠 상점(들)(103)이 소비자 청구서를 취급하지 않는 경우에 요구되며, 이 경우 결제소(들)(105)는 청구서를 취급할 수도 있다.

H. 라이센스 안전한 컨테이너 660 포맷

다음의 표는 BOM과 함께 라이센스 SC(s)(660)에 포함되는 부분을 나타낸다. 키 설명 부분에서 나타낸 바와 같이, 워터마킹 인스트럭션, 컨텐츠(113) 및 컨텐츠(113) 메타데이터를 복호화는데 요구되는 대칭 키(623)는 엔드 유저(들)의 공용키(661)를 이용하여 결제소(들)(105)에 의해 재암호화되었다. 엔드 유저 디바이스(들)(103)가 라이센스 SC(s)(660)를 수신하는 경우, 대칭 키(623)를 복호화하고 이들을 사용하여

라이센스 SC(s)(660) 및 컨텐츠 SC(s)(630)로부터 암호화된 부분을 액세스한다.



다음의 표는 다른 SC(s)에 대해 이전에 설명되지 않은 상기 라이센스 SC(s)(660)에서 사용되는 용어를 설명한다.

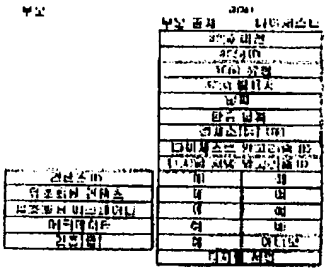
· 엔드 유저 공용키 - 엔드 유저(들)의 공용키(661)가 데이터를 암호화하는데 사용됨을 표시하는 식별자.

· 주문 SC(s)(650) ID - 주문 SC(s)(650) BOM으로부터 취해진 SC(s) ID.

· 인증서 취소 리스트 - 결제소(들)(105)에 의해 이전에 송출되고 서명되었으나, 더 이상 유효한 것으로 간주하지 않는 인증서 ID의 선택사양적인 리스트. 취소 리스트에 포함되는 인증서에 의해 확인될 수 있는 서명을 갖는 임의의 SC(s)는 유효한 SC(s)이다. 엔드 유저 플레이어 애플리케이션(195)은 엔드 유저 디바이스(들)(109)상의 결제소(105) 인증서 취소 리스트의 카피를 저장한다. 취소 리스트가 수신되는 경우, 엔드 유저 플레이어 애플리케이션(195)은 새로운 것으로 것이 갱신되는 경우 그 로컬 카피를 교체한다. 취소 리스트는 리스트가 가장 최근 것임을 결정하기 위해 버전 번호 또는 타임 스탬프(또는 둘 모두)를 포함한다.

I. 컨텐츠 안전한 컨테이너 포맷

다음의 표는 BOM가 함께 컨텐츠 SC(s)(630)에 포함되는 부분을 도시한다.



다음은 다른 SC(s)에 대해 이전에 설명되지 않은 상기 컨텐츠 SC(s)(630)에서 사용된 용어를 설명한다.

· 암호화된 컨텐츠 - 대칭 키(623)를 이용하여 컨텐츠 제공자(들)(101)에 의해 암호화된 컨텐츠(113).

· 암호화된 메타데이터 - 대칭 키(623)를 이용하여 컨텐츠 제공자(들)(101)에 의해 암호화된 컨텐츠(113)와 연관된 메타데이터.

암호화된 부분을 복호화하는데 요구되는 키는 결제소(들)(105)에서 구축되는 라이센스 SC(s)(660)에 있으므로 컨텐츠 SC(s)(630)에 포함되는 키 설명 부분이 존재하지 않는다.

VI. 안전한 컨테이너 패킹 및 언패킹

A. 개요

SC(s) 패커는 모든 지정된 부분을 갖는 SC(s)를 생성하기 위해 다수의 또는 단일의 프로세스 단계에서 호출될 수 있는 애플리케이션 프로그래밍 인터페이스(Application Programming Interface : API)를 갖는 32비트 윈도우즈 프로그램이다. 각종 하드웨어 플랫폼의 SC(s) 패커(151, 152, 153)는 컨텐츠 제공자(들)(101), 결제소(들)(105), 전자 디지털 컨텐츠 상점(들)(103), SC(s) 패킹을 필요로 하는 다른 사이트에서의 윈도우즈 프로그램을 지원한다. BOM 및, 필요하다면, 키 설명 부분은 SC(s)에서 생성되어 포함되어 있다. 패커 API 세트는 호출자가 BOM 및 키 설명 부분의 레코드를 생성하고 SC(s)에 부분을 포함하도록 요구되는 정보를 지정하도록 한다. 다이제스트 및 디지털 서명을 연산하는 것과 함께 부분 및 대칭 키(623)의 암호화는 패커에 의해 또한 수행된다. 패커에 의해 지원되는 암호화 및 다이제스트 알고리즘은 패커 코드에 포함되거나 또는 이들은 외부 인터페이스를 통해 호출된다.

SC(s)를 구축하는 패커에 대한 인터페이스는 입력으로서 다음의 파라미터를 채택하는 API에 의해 행해진다.

· 연결 구조의 버퍼에 대한 포인터. 버퍼의 각 구조는 커맨드를 실행하는데 요구되는 정보를 갖는 패커에 대한 커맨드이다. 패커 커맨드는 연관된 BOM 레코드를 갖는 SC(s)에 부분을 부가하고, BOM에 레코드를 부가하며, 키 설명 부분에 레코드를 부가하는 것을 포함한다.

· 상기 설명된 버퍼에 포함된 연결 구조의 번호를 표시하는 값.

· BOM 부분의 명칭 및 위치.

· 각각의 비트의 값은 정의된 플래그 또는 차후 사용을 위해 예비된 플래그이다. 현재 다음의 플래그가 정의되어 있다.

- 버퍼내의 모든 구조가 프로세스된 후에 SC(s)의 모든 부분이 단일 화일내로 함께 번들되는지의 여부에 대한 표시. 부분을 단일 객체로 번들링하는 것은 SC(s)를 구축하는 경우에 수행되는 최종 단계이다.

- BOM 부분으로부터 디지털 서명이 생략되는지의 여부에 대한 표시. 이 플래그가 설정되지 않는 경우, 디지털 서명은 SC(s)가 단일 객체로 번들링되기 전에 올바르게 연산된다.

다른 실시예에 있어서, 다음과 같은 파라메터를 입력으로서 수용하는 API들에 의해서 SC를 수립하기 위한 패커(packer)로의 인터페이스가 이루어진다.

-먼저, SC BOM 부분에 기록된 IP, BOM 부분에 대해서 사용되는 명칭, 추가될 부분을 찾기 위한 디폴트 위치 및 플래그 값으로서 표시되는 SC 설정을 초기화하는 데 사용되는 정보를 이루는 구조로 포인터내에서 전달함으로써, 자료의 계산서(BOM : Bill of Materials) 부분을 생성하도록 API가 호출된다. 이 API는 다음의 패커 API에서 사용되는 SC 핸들을 반환한다.

- 패커는 부분에 SC가 추가될 때마다 사용되는 API를 구비한다. 이 API는 이전의 패커 API, 추가될 부분에 대해서 정보를 이루는 구조에 대한 포인터 및 플래그 값에 의해서 미리 반환되는 SC 핸들을 수용한다. 추가될 부분에 대한 정보는 그 부분의 명칭 및 위치, 그 부분에 대해서 BOM에서 사용될 명칭, 추가될 부분의 유형, 그 부분에 대한 해시값, 플래그 등을 포함한다.

-모든 부분이 SC에 추가된 후, 패커 API는 BOM 부분을 포함하는 모든 부분을 SC 객체(일반적으로, 파일)로 패키징하도록 요청된다. 이 API는 이전의 패키징된 API에 의해서 반환되는 SC 핸들, 패키징된 SC에 대해 사용될 명칭, SC를 서명하기 위한 정보를 구비하는 구조로의 포인터 및 플래그 값을 수용한다.

패커나 패커라고 칭하는 엔티티 중 하나는 SC 템플릿(template)을 사용해서 SC를 형성할 수 있다. SC 템플릿은 형성될 SC 내에서 요구되는 부분 및 기록을 규정하는 정보를 갖는다. 또한, 템플릿은 대칭키(623) 및 암호화된 부분을 암호화하기 위해서 사용되는 암호화 방법 및 관련 키를 규정할 수 있다.

패커는 SC를 언패키징하기 위해서 사용되는 API를 구비한다. 언패키징은 SC 획득 처리이자 자신의 개별 부분으로 SC를 분리하는 처리이다. 그 다음 패커는 SC로부터 언패키징된 소정의 암호화된 부분을 해독하도록 요청할 수 있다.

B. BOM(Bill of Materials) 부분

BOM 부분은, SC가 구성될 때 패커에 의해서 생성된다. BOM은 SC에 대한 정보의 레코드 및 SC에 포함되는 부분에 대한 정보의 레코드를 포함하는 텍스트 파일이다. BOM 내의 각 레코드는 신규 레코드의 시작을 지시하는 신규 라인을 갖는 단일 라인상에 있다. 대개 BOM은 각 부분에 대한 다이제스트와 SC의 확실성 및 무결성을 확인하는 데 사용될 수 있는 디지털 구조를 포함한다.

BOM 내의 레코드 유형은 다음과 같다.

IP

IP 레코드는 SC에 적합한 값의 쌍인 한 세트의 명칭을 포함한다. 다음과 같은 명칭은 SC의 특정한 특성을 위해서 예약된다.

V major.minor.fix

V 특성은 SC의 버전을 명시한다. 이것은 SC가 생성되는 SC 설명의 버전 수이다. 다음에 오는 문자열은 major.minor.fix일 것이고, 여기에서 major, minor 및 fix는 각가 주 배포수, 소 배포수 및 고정 레벨이다.

ID값

ID 특성은 이 SC를 생성하는 엔티티에 의해서 이 특정 SC로 할당되는 고유 값이다. 그 값의 포맷은 이 명세서의 후반부에서 규정한다.

T값

T 특성은 다음중 하나가 될 SC의 유형을 명시한다.

ORD- 주문 SC(650)

OFF- 제의 SC(641)

LIC- 라이센스 SC

TRA- 트랜잭션 SC(640)

MET-메타 데이터 SC(620)

COM- 컨텐츠 SC(630)

A값

A 특성은 SC의 저자나 출판업자를 밝힌다. 저자/출판업자는 본질적으로 명백한 및/또는 등록된

결제소(105)이어야 한다.

D값

D 특성은 SC가 생성되는 날짜, 시간(선택적임)을 밝힌다. 그 값은 연도/월/일@시간:분:초.초의 소수(시간대)를 나타내는 yyyy/mm/dd[@hh:mm[:ss[.fsec]] [(TZ)]]의 형태이어야 한다. 그 값의 선택적인 부분은 [] 기호내에 집어 넣는다.

E값

E 특성은 SC가 만기되는 날짜, 시간(선택적임)을 밝힌다. 그 값은 이전에 규정된 D 특성에서 사용된 유형과 동일해야 한다. 만기 날짜/시간은 가능할 때마다 결제소(105)에서의 날짜/시간과 비교되어야 한다.

CCURL값

CCURL 특성은 결제소(105)의 URL을 밝힌다. 그 값은 유효한 내부 URL의 형태여야 한다.

H값

H 특성은 SC 내에 포함되는 부분에 대한 메시지 다이제스트를 산출하는 데 사용되는 알고리즘을 밝힌다. 예시적인 다이제스트 알고리즘은 MD5이다.

D

D 레코드는 부분의 유형, 부분의명칭, 부분의 (선택적인)다이제스트, 그 부분이 SC에 포함되지 않는 다는 (선택적인)표시를 나타내는 정보를 포함하는 데이터 또는 부분 엔트리 레코드이다. 유형 식별자의 직후에 있는 A 표시는 그 부분이 SC 내에 포함되지 않는다는 것을 나타내는 데 사용된다. 다음은 데이터의 유형이나 부분 레코드를 예약한다.

K part_name [digest]

키 설명 부분을 명시한다.

W part_name [digest]

워터마킹 명령어 부분을 명시한다.

C part_name [digest]

디지털 서명을 확인하기 위해서 사용되는 인증서를 명시한다.

T part_name [digest]

사용 조건 부분을 명시한다.

VF part_name [digest]

제의 SC(641)에 대한 템플릿(template) 부분을 명시한다.

VO part_name [digest]

주문 SC(650)에 대한 템플릿 부분을 명시한다.

VL part_name [digest]

라이센스 SC(660)에 대한 템플릿 부분을 명시한다.

ID part_name [digest]

참조될 컨텐츠(113) 항목의 컨텐츠(113) ID를 명시한다.

CH part_name [digest]

결제소(105) 인증서 부분을 명시한다.

SP part_name [digest]

전자 디지털 컨텐츠 상점(103) 인증서 부분을 명시한다.

B part_name [digest]

SC 내에 포함된 자신의 부분이나 자신의 부분의 서브세트를 갖는 기타 SC에 대한 BOM 부분을 명시한다.

BP part_name [digest]

SC 내의 단일 부분으로서 포함되는 기타 SC에 대한 BOM 부분을 명시한다. sc_part_name 파라메터는 이 SC 내에 포함되는 SC 부분의 명칭이고, 그것도 이 BOM 부분이 규정한다. 이 것과 동일한 BOM도 sc_part_name 파라메터에 의해서 규정되는 SC 내에 포함된다.

D part_name [digest]

데이터(또는 메타 데이터) 부분을 명시한다.

S

S 레코드는 SC의 디지털 서명을 규정하는 데 사용되는 서명 레코드이다. 이 디지털 서명은 다음과 같이 명기된다.

S key_identifier signature_ string signature_algorithm

S 레코드는 서명의 암호화 키를 나타내는 key_identifier, 디지털 서명 비트열의 암호화 베이스(64)인 signature_ string, 그리고 디지털 서명을 생성하도록 다이제스트를 암호화하는 데 사용되는 signature_algorithm을 포함한다.

C. 키 설명 부분

키 설명 부분은 SC 암호화된 부분의 해독에 필요한 암호화 키에 대한 정보를 제공하는 패커에 의해서 생성된다. 암호화된 부분은 형성될 SC 내에 포함되거나 형성될 SC에 의해서 참조되는 기타 SC 내에 포함될 수도 있다. 키 설명 부분은 암호화 키 및 암호화 키가 사용되는 부분에 대한 정보의 레코드를 포함하는 텍스트 파일이다. 키 설명 부분 내의 각 레코드는 신규 레코드의 개시를 나타내는 신규 라인과 단일 라인에 있다.

다음 레코드 유형은 키 설명 부분 내에서 사용되고 다음과 같이 규정된다.

K

encrypted_part_name; result_part_name; part_algorithm_identifier; public_key_identifier

key_encryption_algorithm 및 encrypted_symmetric_key

K 레코드는 이 SC 내에 포함되거나 이 레코드에 의해서 참조되는 다른 SC 내에 포함될 수 있는 암호화된 부분을 명시한다. encrypted_part_name은 이 SC 내의 부분 명칭이거나 다른 SC 내의 암호화된 부분의 명칭을 나타내는 URL이다. result_part_name은 해독된 부분에 부여되는 명칭이다. part_algorithm_identifier는 부분을 암호화하는 데 사용된 암호화 알고리즘을 나타낸다. public_key_identifier는 대칭키(623)을 암호화하는 데 사용된 키의 식별자이다.

key_encryption_algorithm은 대칭키(623)을 암호화하는 데 사용된 암호화 알고리즘을 나타낸다. encrypted_symmetric_key는 부분을 암호화하는 데 사용된 암호화된 대칭키(623) 비트 열을 암호화하는 베이스(64)이다.

VII. 결제소(105)

A. 개요

결제소(105)는 안전한 디지털 컨텐츠 전자 배포 시스템(100)의 권리 관리 기능에 대한 책임이 있다. 결제소(105) 기능은 전자 디지털 컨텐츠 상점(103)의 권리 부여, 컨텐츠(113)에 대한 권리의 확인, 트랜잭션 및 관련 정보의 매입, 엔트 유저 장치(109)에 대한 컨텐츠 암호화 키 또는 대칭 키(623)의 배포, 그들 키의 배포 추적, 그리고 전자 디지털 컨텐츠 상점(103) 및 컨텐츠 제공자(101)에 대한 트랜잭션 개요의 보고의 무결성 및 확실성의 확인을 포함한다. 컨텐츠 암호화 키는 엔드 유저 장치(109)에 의해서 사용되어 권리 획득자에 대해 컨텐츠의 잠금을 해제하며, 권리 획득자는 일반적으로 인증된 전자 디지털 컨텐츠 상점(103)으로부터 구입하여 권리를 획득한다. 컨텐츠 암호화 키가 엔드 유저 장치(109)로 전송되기 전에, 결제소(105)는 컨텐츠(113) 및 엔드 유저 장치(109)가 컨텐츠(113)를 보유할 권리를 판매하는 엔티티의 확실성을 확인하는 확인 처리를 통해서 수행한다. 이것은 SC 분석 툴(185)이라고 칭해진다. 또한, 몇몇 구성에 있어서, 결제소(105)는 컨텐츠(113) 구입의 재정 결산을, 신용 카드 인증 및 계산서 발송의 전자 디지털 컨텐츠 상점(103) 기능을 수행하는 결제소(105)에 함께 배치된 시스템에 의해서 처리할 수도 있다. 결제소(105)는 IC검증(ICVerify) 및 과세 소프트웨어(Taxware)와 같은 OEM 패키지를 사용해서 신용 카드 처리 및 로컬 판매 과세를 취급한다.

전자 디지털 컨텐츠 상점 구현

안전한 디지털 컨텐츠 전자 배포 시스템(100)에서 컨텐츠(113)의 판매자로서 참여하기를 원하는 전자 디지털 상점(103)은, 안전한 디지털 컨텐츠 전자 배포 시스템(100)으로 컨텐츠(113)를 제공하는 하나 이상의 디지털 컨텐츠 제공자(101)를 요청한다. 두 부분이 계약되기만 하면 요청의 처리는 한정되지 않는다. 뮤직 라벨(Music Label), 예를 들어, 소니(Sony), 타임 워너(Time-Warner) 등과 같은 디지털 컨텐츠 라벨이 전자 디지털 컨텐츠 상점(103)이 자신의 컨텐츠(113)를 팔도록 결정한 후, 결제소(105)는 전자 디지털 컨텐츠 상점(103)이 안전한 디지털 컨텐츠 전자 배포 시스템(100)에 추가되길 원하는 요청에 (대개, 전자 우편을 통해서)접할 것이다. 디지털 컨텐츠 라벨은 전자 디지털 컨텐츠 상점(103)의 명칭 및 결제소(105)가 그 전자 디지털 컨텐츠 상점(103)에 대한 디지털 인증서를 생성하는 데 필요한 기타 정보를 제공한다. 디지털 인증서는 안전한 유형으로 디지털 컨텐츠 라벨에 전송된 후, 디지털 컨텐츠 라벨에 의해서 전자 디지털 컨텐츠 상점(103)으로 발송된다. 결제소(105)는 할당된 디지털 인증서의 데이터 베이스를 유지한다. 각 인증서는 버전 수, 고유 일련 번호, 서명 알고리즘, 발행인의 명칭(예를 들어, 결제소(105)의 명칭), 인증서가 유효 기간, 전자 디지털 컨텐츠 상점(103)의 명칭, 전자 디지털 컨텐츠 상점(103)의 공용키(621), 그리고 결제소(105)의 사설 키를 사용하여 서명된 모든 기타 정보의 해시 코드를 포함한다. 결제소(105)의 공용키(621)를 구비하는 엔티티는 인증서를 확인할 수 있고, 그 후, 유효 SC인 인증서로부터의 공용키를 사용해서 인증될 수 있는 서명을 갖는 SC를 확신할 수 있다.

전자 디지털 컨텐츠 상점(103)은 결제소(105)에 의해서 생성된 자신의 디지털 인증서 및 디지털 컨텐츠 라벨로부터의 SC를 처리하기 위한 필수 툴을 수신한 후, 엔드 유저에 의해서 구입될 수 있는 컨텐츠(113)의 제공을 시작할 수 있다. 전자 디지털 컨텐츠 상점(103)은 자신의 인증서 및 트랜잭션 SC(640)을 포함하고, 자신의 디지털 서명(643)을 사용하는 SC를 승인한다. 엔드 유저 장치(109)는, 먼저 디지털 인증서 취소 목록을 체크한 후, 결제소(105)의 공용키(621)를 사용하여 전자 디지털 컨텐츠 상점(103)에 대한 디지털 인증서 내의 정보를 확인함으로써, 전자 디지털 컨텐츠 상점(103)이 안전한 디지털 컨텐츠 전자 배포 시스템(100) 상의 확인된 컨텐츠(113)의 배포자인지를 확인한다. 디지털 인증서 취소 목록은 결제소(105)에 의해서 유지된다. 취소 목록은 결제소(105)에 의해서 생성된 라이센스 SC(660) 내의 일부분으로서 포함될 수도 있다. 엔드 유저 장치(109)는 전자 디지털 컨텐츠 상점(103) 디지털 인증서 확인

부분으로서 사용할 수 있도록 엔드 유저 장치(109) 상의 취소 목록 사본을 보존한다. 엔드 유저 장치(109)는 라이센스 SC(660)을 수신할 때마다, 새로운 취소 목록이 포함되어 있는 지를 판정하고, 만일 포함되어 있다면, 엔드 유저 장치(109) 상의 로컬 취소 목록을 갱신한다.

8. 권리 관리 처리

주문 SC 분석

엔드 유저가 전자 디지털 컨텐츠 상점(103)으로부터 제의 SC(641)를 포함하는 트랜잭션 SC(640)를 수신한 후, 결제소(105)는 엔드 유저로부터 주문 SC(650)를 수신한다. 주문 SC(650)는 컨텐츠 및 자신의 사용에 관련된 정보 부분, 컨텐츠(113)를 판매하는 전자 디지털 컨텐츠 상점(103)에 대한 정보 부분 및 컨텐츠(113)를 구입하는 엔드 유저에 대한 정보 부분으로 이루어진다. 결제소(105)는 주문 SC(650) 내의 정보를 처리하기 전에, SC가 실제 유효하고 어떠한 방식으로도 부도덕하지 않은 데이터를 포함하는 지를 보증하는 몇몇 절차를 먼저 수행한다.

유효성 확인(validation)

결제소(105)는 디지털 서명을 확인하여 주문 SC(650)의 유효성 확인하기 시작해서, 주문 SC(650) 부분의 무결성을 확인한다. 디지털 서명을 확인하기 위해서, 제소(105)는, 만일 서명되어 있다면 그 서명을 포함하는 서명된 엔티티의 공용키(661)를 사용해서 자신의 서명 컨텐츠(631)를 먼저 해독한다. (사인된 엔티티는 컨텐츠 제공자(101), 전자 디지털 컨텐츠 상점(103), 엔드 유저 장치(109) 또는 그들의 소정 조합일 수 있다.) 그 다음, 결제소(105)는 SC의 산출된 부분 다이제스트의 다이제스트를 산출하고, 그것을 해독된 컨텐츠(113)로부터의 디지털 서명과 비교한다. 두 값이 일치하면, 디지털 서명은 유효하다. 각 부분의 무결성을 확인하기 위해서, 결제소(105)는 그 부분의 다이제스트를 산출하고, 그것을 BOM 내의 다이제스트 값과 비교한다. 이후, 결제소(105)는 동일한 처리를 수행하여 디지털 서명과 주문 SC(650) 내에 포함되는 메타 데이터 및 제의 SC(641) 부분에 대한 부분 무결성를 확인한다.

트랜잭션 및 제의 SC(641) 디지털 서명의 유효성 확인 처리도, 전자 디지털 컨텐츠 상점(103)이 안전한 디지털 컨텐츠 전자 배포 시스템(100)에 의해서 인증되었다는 것을 간접적으로 확인한다. 이것은, 결제소(105)가 인증서의 발행인이라는 사실에 기초한다. 그 대신에, 결제소(105)가 전자 디지털 컨텐츠 상점(103)으로부터의 공용키를 사용해서 트랜잭션 SC(640) 및 제의 SC(641)의 디지털 서명을 연속적으로 확인할 수 있지만, 단지 SC를 서명하는 엔티티가 관련 사설키의 소유권을 갖는 경우에만 그렇다. 전자 디지털 컨텐츠 상점(103)만이 관련 사설키의 소유권을 갖는다. 결제소(105)가 전자 디지털 컨텐츠 상점(103)의 로컬 데이터 베이스를 가질 필요가 없다는 점에 주의하라. 상점은 결제소 공용키를 사용해서 트랜잭션 SC(640) 제의 SC(641) 공용키를 서명하기 때문이다.

그 다음, 유저 장치가 구입하는 컨텐츠(113)의 상점 사용 조건(519)은 결제소에 의해서 확인되어 그들이 메타 데이터 SC(620) 내에 설정된 사양 내에서 있도록 보장한다. 메타 데이터(620)가 주문 SC(650) 내에 포함되는 점을 상기하라.

키 처리

암호화된 대칭키(623)의 처리 및 워터마킹 명령의 처리는, 주문 SC(650)의 확실성 및 무결성 체크, 전자 디지털 컨텐츠 상점(103)의 유효성 확인 및 상점 사용 조건(519)의 유효성 확인이 연속적으로 완료된 후, 결제소(105)에 의해서 이루어진다. 일반적으로, 주문 SC(650)의 메타 데이터 SC(620) 부분은, 결제소(105)의 공용키(621)를 사용해서 암호화되는 키 설명 부분에 배치된 몇몇 대칭 키(623)를 구비한다. 대칭키(623)의 암호화는 메타 데이터 SC(620)가 생성될 때 컨텐츠 제공자(101)에 의해서 이루어진다.

소정 대칭키(623)는 워터마킹 명령 및 컨텐츠(113)를 해독하기 위한 기타 명령어, 그리고 소정 암호화된 메타 데이터를 해독하는 데 사용된다. 컨텐츠(113)는 한 곡의 노래나 CD 상의 전체 노래 모음을 나타낼 수 있기 때문에, 각 노래에 대해서 상이한 대칭 키(623)가 사용될 수도 있다. 워터 마킹 명령은 주문 SC(650)의 메타 데이터 SC(620) 부분 내에 포함된다. 컨텐츠(113) 및 암호화된 메타 데이터는, 컨텐츠 호스팅 사이트(111)에서 컨텐츠 SC(630) 내에 있다. 컨텐츠 SC(630) 내의 암호화된 컨텐츠(113)의 URL 및 부분 명칭과 메타 데이터 부분은, 주문 SC(650)의 메타 데이터 SC(620) 부분의 키 설명 부분에 포함된다. 결제소(105)는 자신의 사설키를 사용해서 대칭 키(623)를 해독한 후, 엔드 유저 장치(109)의 공용키(661)를 사용해서 그 해독된 대칭 키 각각을 암호화한다. 엔드 유저 장치(109)의 공용키(661)는 주문 SC(650)로부터 검색된다. 새로 암호화된 대칭키(623)는 결제소(105)가 엔드 유저 장치(109)로 반환하는 라이센스 SC(660)의 키 설명 부분에 포함된다.

대칭 키(623) 처리 시간 동안에, 결제소(105)는 워터마킹 명령으로 변형하길 원할 수도 있다. 그러한 이유라면, 결제소(105)가 대칭키(623)를 해독한 후, 워터마킹은 변형 및 재암호화될 것이다. 신규 워터마킹 명령은 엔드 유저 장치(109)로 반환될 라이센스 SC(660) 내의 부분중 하나로서 포함된다.

모든 주문 SC(650)의 처리가 성공하면, 결제소(105)는 엔드 유저 자치(109)로 라이센스 SC(660)를 반환한다. 엔드 유저 장치(109)는 라이센스 SC(660) 정보를 사용해서 컨텐츠 SC(630)을 다운로드 받고, 암호화된 컨텐츠(113) 및 메타 데이터에 액세스한다. 또한, 워터마킹 명령어는 엔드 유저 장치(109)에 의해서 실행된다.

결제소(들)(105)가 주문 SC(s)(650)를 성공적으로 처리할 수 없는 경우, HTML 페이지가 엔드 유저 장치(들)(109)로 반환되고 인터넷 브라우저 윈도우에서 디스플레이된다. HTML 페이지는 결제소(들)(105)가 트랜잭션을 처리할 수 없었던 이유를 나타낸다.

대안적인 실시예에서, 사용자가 판매를 위해 설정된 데이터를 발매하기 이전에 컨텐츠(113)의 카피를 구입한 경우, 대칭 키(623)없이 라이센스(들) SC(660)가 반환된다. 대칭 키(623)를 수신하기 위해 데이터를 발매시 또는 발매후에 라이센스(들) SC(660)가 결제소(들)(105)로 반환된다. 예로서, 컨텐츠 제공자(들)(101)는 노래에 대한 데이터를 발매하기 이전에 사용자가 새로운 노래를 다운로드하도록 허용함으로써, 고객이 노래를 다운로드하고, 컨텐츠 제공자(들)(101)에 의해 설정된 데이터 이전에 노래를 재

생할 준비를 할 수 있도록 한다. 이것은 발매 데이터에 대한 대역폭 및 다운로드 시간에 대한 컨텐츠를 갖지 않고서도, 발매 데이터에 대한 컨텐츠(113)의 즉각적인 개시를 허용한다.

C. 국가 특정 파라메타(Country Specific Parameters)

선택적으로, 결제소(들)(105)는 엔드 유저 장치(들)(109)의 도메인 이름을 사용하며, 가능한 때라면 언제라도, 신용 카드 계산서 발송 어드레스를 사용함으로써, 엔드 유저(들)의 국가 위치를 결정한다. 엔드 유저(들)가 거주하는 국가에서 컨텐츠(113)를 판매하는데 어떠한 제한 사항이 있는 경우, 결제소(들)(105)는 라이센스 SC(660)를 엔드 유저 장치(들)(109)로 전송하기 이전에, 처리되고 있는 트랜잭션이 그러한 제한 사항들 중 어느 것도 위반하지 않음을 보장한다. 또한, 전자 디지털 컨텐츠 상점(들)(103)은 결제소(들)(105)와 동일한 체크를 수행함으로써 컨텐츠(113)를 여러 국가들로 배포하는 것을 관리하는데 참여할 것으로 예상된다. 결제소(들)(105)는 전자 디지털 컨텐츠 상점(들)(103)이 컨텐츠 제공자(들)(101)에 의해 설정된 국가 특정 규칙을 무시하는 경우에 할 수 있는 모든 체크를 수행한다.

D. 회계 감사 로그 및 트랙킹(Audit Logs and Tracking)

결제소(들)(105)는 컨텐츠(113) 구입 트랜잭션 및 보고 요구 트랜잭션 동안 수행되는 각각의 동작에 대한 정보의 회계 감사 로그(150)를 유지한다. 정보는 안전한 디지털 컨텐츠 전자 배포 시스템(100)의 회계 감사, 보고의 생성, 데이터 마이닝(mining)과 같은 다양한 목적으로 사용될 수 있다.

또한, 결제소(들)(105)는 전자 디지털 컨텐츠 상점(들)(103)에 대한 계산서 발송 서브시스템(182) 내에 계정 대조(account balance)를 유지시킨다. 디지털 컨텐츠 레이블에 의해 전자 디지털 컨텐츠 상점(들)(103)에 대한 프라이싱(pricing) 구조가 결제소(들)(105)에 제공된다. 이러한 정보는 현재의 특별사항, 볼륨 디스카운트, 전자 디지털 컨텐츠 상점(들)(103)에 부과될 필요가 있는 계정 부족액 한계와 같은 것을 포함할 수 있다. 결제소(들)(105)는 전자 디지털 컨텐츠 상점(들)(103)의 대조를 트랙킹하기 위해 프라이싱 정보를 사용하며, 그들이 컨텐츠 제공자(들)(101)에 의해 설정된 그들의 부족액 한계를 초과하지 않도록 보장한다.

전형적으로, 결제소(들)(105)에 의해 이하의 동작들이 로그된다.

- 라이센스 SC(s)(660)에 대한 엔드 유저 장치(들)(109) 요구.
- 결제소(들)(105)가 계산서 발송을 처리시의 신용 카드 인증 번호.
- 엔드 유저 장치(들)(109)에 대한 라이센스 SC(s)(660) 분배.
- 보고에 대한 요구.
- 컨텐츠 SC(630) 및 라이센스 SC(s)(660)가 수신 및 유효화되었던 엔드 유저(들)로부터의 통지.

전형적으로, 라이센스 SC(660)에 대한 결제소(들)(105)에 의해 이하의 정보가 로그된다.

- 요구의 일자 및 시간.
- 구입 트랜잭션의 일자 및 시간.
- 구입되는 항목의 컨텐츠 ID.
- 컨텐츠 제공자(들)(101)의 식별.
- 상점 사용 조건(519).
- 워터마킹 인스트럭션 변형.
- 전자 디지털 컨텐츠 상점(들)(103)에 의해 부가되었던 트랜잭션 ID(535).
- 전자 디지털 컨텐츠 상점(들)(103)의 식별.
- 엔드 유저 장치(들)(109)의 식별.
- (결제소(들)(105)가 계산서를 발송을 처리하는 경우의) 엔드 유저 신용 카드 정보.

전형적으로, 엔드 유저 신용 카드 유효를 위해 결제소(들)(105)에 의해 이하의 정보가 로그된다.

- 요구의 일자 및 시간.
- 신용 카드에 부과된 총액.
- 구입되는 항목의 컨텐츠 ID.
- 전자 디지털 컨텐츠 상점(들)(103)에 의해 부가되었던 트랜잭션 ID(535).
- 전자 디지털 컨텐츠 상점(들)(103)의 식별.
- 엔드 유저(들)의 식별.
- 엔드 유저(들) 신용 카드 정보.
- 신용 카드의 클리어러(clearer)로부터 수신된 인증 번호.

전형적으로, 라이센스 SC(s)(660)가 엔드 유저 장치(들)(109)로 전송될 때 결제소(들)(105)에 의해 이하의 정보가 로그된다.

- 요구의 일자 및 시간.

- 구입되는 항목의 컨텐츠 ID.
- 컨텐츠 제공자(들)(101)의 식별.
- 사용 조건(517).
- 전자 디지털 컨텐츠 상점(들)(103)에 의해 부가되었던 트랜잭션 ID(535).
- 전자 디지털 컨텐츠 상점(들)(103)의 식별.
- 엔드 유저(들)의 식별.

전형적으로, 보고 요구가 만들어질 때 이하의 정보가 로그된다.

- 요구의 일자 및 시간.
- 보고가 전송된 일자 및 시간.
- 요구되는 보고의 타입.
- 보고를 생성하는데 사용된 파라메타.
- 보고를 요구하는 엔티티의 식별자.

E. 결과의 보고

엔드 유저(들) 구입 트랜잭션 동안 결제소(들)(105)가 로그한 정보를 이용하여 결제소(들)(105)에 의해 보고가 생성된다. 컨텐츠 제공자(들)(101) 및 전자 디지털 컨텐츠 상점(들)(103)은 결제소(들)(105)로부터 지불 입증 인터페이스(183)를 경유하여 트랜잭션 보고를 요구할 수 있으므로, 그들은 결제소(들)(105)에 의해 로그된 정보를 갖는 그들 자신의 트랜잭션 데이터베이스를 조정할 수 있다. 또한, 결제소(들)(105)는 컨텐츠 제공자(들)(101) 및 전자 디지털 컨텐츠 상점(들)(103)으로 주기적인 보고를 제공할 수 있다.

결제소(들)(105)는 컨텐츠 제공자(들)(101) 및 전자 디지털 컨텐츠 상점(들)(103)이 보고를 요구 및 수신할 수 있도록 하는 안전한 전자 인터페이스를 정의한다. 보고 요구 SC(s)는 결제소(들)(105)에 의해, 요구를 시작하는 엔티티로 할당된 인증서를 포함한다. 결제소(들)(105)는 증명서 및 SC 디지털 서명을 이용하여 인증된 엔티티로부터 발생된 요구를 입증한다. 또한, 요구는 보고의 영역을 정의하는, 지속 시간(time duration)과 같은 파라메타를 포함한다. 결제소(들)(105)는 요구자들로 하여금 요구자 자신들이 갖도록 허용된 정보만을 수신하도록 보장하기 위해 요구 파라메타를 유효화한다.

결제소(들)(105)가 보고 요구 SC(s)가 인증 및 유효한 것으로 결정한 경우, 결제소(들)(105)는 보고를 생성한 후, 그것을 요구를 시작한 엔티티로 전송될 보고 SC(s) 내로 패킹한다. 일부 보고는 정의된 시간 간격에서 자동으로 생성되고, 결제소(들)(105)에 저장될 수 있으므로, 보고는 요구가 수신될 때 즉각적으로 전송될 수 있다. 보고 내에 포함된 데이터의 포맷은 본 서류의 차후의 버전에서 정의된다.

F. 계산서 발송 및 지불 확인

컨텐츠(113)의 계산서 발송은 결제소(들)(105) 또는 전자 디지털 컨텐츠 상점(들)(103)에 의해 처리될 수 있다. 결제소(들)(105)가 전자 컨텐츠(113)의 계산서 발송을 처리하는 경우, 전자 디지털 컨텐츠 상점(들)(103)은 엔드 유저(들)의 주문을 전자 상품, 만약 적용가능하다면 물리적 상품으로 분리시킨다. 그 후, 전자 디지털 컨텐츠 상점(들)(103)은 엔드 유저(들)의 계산서 발송 정보 및 인증될 필요가 있는 전체 양을 포함하는 트랜잭션의 결제소(들)(105)에 통지한다. 결제소(들)(105)는 엔드 유저(들)의 신용 카드를 인증한 후, 전자 디지털 컨텐츠 상점(들)(103)으로 통지를 다시 반환한다. 결제소(들)(105)가 엔드 유저(들)의 신용 카드를 인증하는 것과 동시에, 전자 디지털 컨텐츠 상점(들)(103)은 구입되는 소정의 물리적 상품에 대해 엔드 유저(들)의 신용 카드를 부과할 수 있다. 엔드 유저 장치(들)(109)에 의해 각각의 전자 항목이 다운로드된 후, 결제소(들)(105)는 엔드 유저(들)의 신용 카드에 부과할 수 있음을 통지받는다. 이것은 컨텐츠(113)가 엔드 유저 장치(들)(109)에서의 사용을 위해 인에이블되기 전에 엔드 유저 장치(들)(109)에 의해 마지막 단계로서 발생된다.

전자 디지털 컨텐츠 상점(들)(103)이 전자 컨텐츠(113)의 계산서 발송을 처리하는 경우, 엔드 유저 장치(들)(109)가 주문 SC(s)(650)를 결제소(들)(105)로 전송할 때까지 결제소(들)(105)는 트랜잭션에 관해 통지받지 않는다. 결제소(105)는 각각의 전자 항목이 다운로드된 후에도 엔드 유저 장치(들)(109)에 의해 여전히 통지받는다. 결제소(들)(105)가 통지를 받을 때, 결제소(들)(105)는 통지를 전자 디지털 컨텐츠 상점(들)(103)으로 전송함으로써, 전자 디지털 컨텐츠 상점(들)(103)이 엔드 유저(들)의 신용 카드를 부과할 수 있도록 한다.

G. 재전송

안전한 디지털 컨텐츠 전자 분배 시스템(100)은 컨텐츠(113)의 재전송을 처리할 수 있는 능력을 제공한다. 이것은 전형적으로 고객 서비스 인터페이스(184)에 의해 수행된다. 전자 디지털 컨텐츠 상점(들)(103)은 엔드 유저가 재전송을 시작하기 위해 진행할 수 있는 사용자 인터페이스를 제공한다. 엔드 유저(들)는 컨텐츠(113)의 재전송을 요구하기 위해, 컨텐츠(113) 항목이 구입되었던 전자 디지털 컨텐츠 상점(들)(103) 사이트로 들어간다.

컨텐츠(113)는 다운로드될 수 없거나 또는 다운로드 되었던 컨텐츠(113)는 사용할 수 없으므로, 컨텐츠(113)의 재전송은 엔드 유저(들)가 이전에 구입된 컨텐츠(113) 항목의 새로운 카피를 요구할 때 행해진다. 전자 디지털 컨텐츠 상점(들)(103)은 컨텐츠(113)의 재전송 권한이 엔드 유저(들)에게 부여될지의 여부에 대해 결정한다. 엔드 유저(들)에게 재전송 권한이 부여된다면, 전자 디지털 컨텐츠 상점(들)(103)은 재전송되는 컨텐츠(113) 항목(들)의 제의 SC(s)(641)를 포함하는 트랜잭션 SC(s)(640)를 형성한다. 트랜잭션 SC(s)(640)는 엔드 유저 장치(들)(109)로 전송되며, 구입 트랜잭션에서와 같은 동일한

단계들이 엔드 유저(들)에 의해 수행된다. 엔드 유저 장치(들)(109)가 재전송을 겪고 있는 컨텐츠(113) 항목(들)에 대한 키 라이브러리 내에 스크램블된 키(들)를 갖는다면, 트랜잭션 SC(s)(640)는 엔드 유저 장치(들)(109)가 스크램블된 키(들)를 삭제하도록 지시하는 정보를 포함한다.

결제소(들)(105)가 컨텐츠(113) 구입의 재정적 해결을 처리하는 경우, 전자 디지털 컨텐츠 상점(들)(103)은 결제소(들)(105)에 전달되는 트랜잭션 SC(s)(640) 내의 플래그를 주문 SC(s)(650) 내에 포함한다. 결제소(들)(105)는 주문 SC(s)(650) 내의 플래그를 해석한 후, 컨텐츠(113)의 구입을 위한 엔드 유저(들)를 변경하지 않고서 트랜잭션을 진행한다.

VIII. 컨텐츠 제공자

A. 개요

안전한 디지털 컨텐츠 전자 배포 시스템(100)에서의 컨텐츠 제공자(들)(101)는 디지털 컨텐츠 레이블이거나 또는 컨텐츠(113)에 대한 권리를 소유한 엔티티이다. 컨텐츠 제공자(들)(101)의 역할은 분배를 위한 컨텐츠(113)를 준비하고, 전자 디지털 컨텐츠 상점(들)(103) 또는 컨텐츠(113)의 다운로드가능 전자 버전의 소매상에게 이용가능한 컨텐츠(113)에 관한 정보를 만드는 것이다. 컨텐츠 제공자(들)(101)에 대한 최상의 보안성 및 권리 제어를 제공하기 위해, 일련의 툴이 제공되어 컨텐츠 제공자(들)(101)가 그들의 전제부에서 그들의 컨텐츠(113)를 준비 및 SC(s) 안으로 안전하게 패키징할 수 있도록 함으로써, 컨텐츠(113)가 컨텐츠 제공자(들)의 도메인을 떠날 때 안전하게 되도록 하고, 비인증자에 의해 결코 노출 또는 액세스되는 일이 없도록 한다. 이것은 컨텐츠(113)가 인터넷과 같은 안전하지 않은 네트워크를 통해, 해커 또는 비인증자에게 노출될지도 모를 우려없이 자유롭게 배포될 수 있도록 한다.

컨텐츠 제공자(들)(101)에 대한 툴의 최종 목표는 노래 또는 일련의 노래와 같은 컨텐츠(113)를 준비 및 컨텐츠 SC(s)(630)로 패키징하며, 노래, 노래의 허가된 사용(컨텐츠 사용 조건(517)), 노래에 대한 판촉 정보를 기술하는 정보를 메타데이터 SC(s)(620) 안으로 패키징하는 것이다. 이를 달성하기 위해, 아래와 같은 툴들의 세트가 제공된다.

- 작업 흐름 관리자(154) : 처리 활동을 스케쥴링하고, 요구되는 처리의 등기화를 관리한다.

- 컨텐츠 처리 툴(155) : 워터마킹, 전처리(오디오를 예로 들면, 소정의 요구되는 등화, 동적 조정 또는 리샘플링), 인코딩 및 압축을 포함하는 컨텐츠(113) 파일 준비를 제어하는 툴의 집합체.

- 메타데이터 동화 및 진입 툴(161) : 컨텐츠 제공자(들)의 데이터베이스(160) 및/또는 제 3자 데이터베이스 또는 데이터 임포트(Import) 파일로부터 및/또는 오퍼레이터 상호작용을 통한 컨텐츠(113) 기술 정보를 모으는데 사용되는 툴의 집합체이며, 컨텐츠 사용 조건(517)을 지정하는 수단을 제공한다. 또한, CDS 또는 DDP 파일에 대한 디지털 오디오 컨텐츠와 같은 컨텐츠를 캡처 또는 추출하는 인터페이스가 제공된다. 품질 제어 툴은 준비된 컨텐츠 및 메타데이터의 미리 보기를 가능하게 한다. 메타데이터에 필요한 소정의 정정 또는 또다른 처리를 위한 컨텐츠의 재의뢰(resubmission)가 행해질 수 있다.

- SC 패커 툴(152) : 모든 컨텐츠(113) 및 정보를 암호화 및 패키징하고, SC 패커를 호출하여 SC(s) 안으로 패키징한다.

- 컨텐츠 분배 툴(도시되지 않음) : 컨텐츠 호스팅 사이트(들)(111) 및 전자 디지털 컨텐츠 상점(들)(103)과 같은 지정된 분배 센터로 SC(s)를 분배한다.

- 컨텐츠 판촉 웹 사이트(156) - 인증된 전자 디지털 컨텐츠 상점(들)(103)에 의한 다운로드를 위해, 메타데이터 SC(s)(620) 및 선택적으로 부가적인 판촉물을 저장한다.

B. 작업 흐름 관리자(154)

이 툴의 목적은 컨텐츠(113) 처리 활동을 스케쥴링, 트랙킹 및 관리하는 것이다. 이 애플리케이션은 멀티 유저 액세스가 가능하게 할 뿐만 아니라 컨텐츠 제공자(들)(101)의 인터넷 또는 엑스트라넷 내의 원격지로부터 컨텐츠(113) 스케쥴링 및 상태 체크를 허용한다. 또한, 이 설계는 공동 처리를 가능하게 함으로써, 다수의 개인들이 다수의 컨텐츠(113) 상에서 병렬로 작업할 수 있고, 서로 다른 개인들에게 특정 책임이 할당될 수 있도록 하며, 이들 개인은 전세계에 걸쳐 널리 퍼져있다.

도 8은, 도 7에 대응하는 작업 흐름 관리자(154)의 주요 처리를 도시하는 블록도이다. 도 8에서의 주요 처리는 이 섹션에서 기술된 툴에 의해 제공되는 컨텐츠(113) 처리 기능을 요약하고 있다. 작업 흐름 관리자(154)는 이를 처리에 잡(job)을 공급하고, 그 현재의 처리를 완료시 잡을 다음의 요구되는 처리로 전달할 책임을 갖는다. 이것은 일련의 애플리케이션 프로그래밍 인터페이스(Application Programming Interface; API)를 통해 수행되며, API 각각은

- 처리를 위한 다음 잡을 만듦,

- 처리의 성공적 완료를 지시,

- 처리의 비성공적 완료 및 그러한 실패의 이유를 지시,

- (단지 의존적 처리의 부분적 완료만을 요구하는 처리들의 시작을 허용하기 위해) 처리의 중간 상태를 제공,

- 지정된 처리에 이용가능하게 만들어진 제품에 코멘트를 부가

하기 위해 툴 호출을 처리한다.

또한, 작업 흐름 관리자(154)는 사용자 인터페이스를 가지며, 예로써 작업 흐름 관리자 사용자 인터페이스(700)가 도 7에 예시되어 있고, 다음과 같은 기능들을 제공한다.

- 처리의 여러 단계를 동안 할당 및 수행될 디폴트 값 및 조건의 지정을 허용하는 구성

패널(configuration panel).

- 작업 흐름 규칙 및 자동화된 처리 흐름의 고객화.

- 잡 스케쥴링.

- 상태 질문 및 보고.

- 하나 이상의 처리와 관련된 잡에 대한 코멘트 또는 인스트럭션 부가.

- 잡 관리(즉, 중지, 해제, 제거, (처리의) 우선순위 변경.

각각의 처리는 작업 흐름 관리자(154)에 의해 관리되는 관련된 큐(queue)를 갖는다. 작업 흐름 관리자(154)로부터 잡을 요구하는 모든 처리는 그 관련된 큐에 현재 잡이 없는 경우 대기 상태에서 처리(들)를 중지하거나, 또는 그 각각의 처리를 수행할 것이 필요한 잡에 관한 모든 정보의 처리를 반환하는 작업 흐름 관리자(154)이다. 처리가 대기 상태에서 중지되는 경우, 작업 흐름 관리자(154)에 의해 잡이 큐 상에 위치될 때 처리를 재개한다.

또한, 작업 흐름 관리자(154)는 정의된 규칙의 세트를 기초로 하여 처리의 흐름 또는 순서를 관리한다. 이들 규칙은, 특별한 처리 요구를 갖거나 또는 특정 디폴트 규칙을 구성하는 경우, 컨텐츠 제공자(들)(101)에 의해 고객화될 수 있다. 처리가 그의 할당된 태스크의 종료를 보고할 때, 이 상태의 작업 흐름 관리자(154)에게 통지하고, 작업 흐름 관리자(154)는 정의된 규칙을 기초로 하여 잡이 다음에 위치할 큐를 결정한다.

특별한 처리 인스트럭션 또는 통지를 지시하는 코멘트가 소정의 처리 단계에서 프로그래밍 API를 통해, 또는 작업 흐름 관리자 사용자 인터페이스(700) 혹은 프로세서 인터페이스를 통해 수동적으로 제품에 부착될 수 있다.

작업 흐름 관리자(154) 내의 처리는 바람직한 실시예의 경우 자바(Java)로 구현되지만, C/C++, 어셈블러와 같은 다른 프로그래밍 언어를 사용하여 구현될 수도 있다. 작업 흐름 관리자(154)에 대해 이하 기술된 처리는 다양한 하드웨어 및 소프트웨어 플랫폼 상에서 실행될 수 있다. 완성 시스템으로서 또는 그의 구성 프로세스를 중 어느 하나로서의 작업 흐름 관리자(154)는 웹 또는 온 플로피 디스켓, CD ROM 및 제거가능 하드 디스크 드라이브(이들에 제한되지는 않음)와 같은 전자 배포를 포함하는 컴퓨터 판독가능 매체 내에 애플리케이션 프로그램으로서 배포될 수 있다.

도 8은, 도 7에 대응하는 작업 흐름 관리자(154)의 주요 처리의 블록도이다. 이하의 섹션은 각각의 처리를 요약한 것이며, 각각의 처리에서 요구되는 정보 또는 동작을 기술한다.

1. 제품 대기 동작/정보 처리(801)

해당 처리에 의해 요구되는 모든 정보가 이용가능하면 잡은 특정 처리 큐에 위치하게 되며, 잡은 모든 의존적 처리를 이미 성공적으로 완료하였다. 작업 흐름 관리자(154) 내에는 특별한 큐가 존재하며, 이것은 정보를 잃어버리거나 혹은 또다른 처리를 방해하는 실패로 인해 현재 처리에 이용가능하지 않은 잡을 유지하는데 사용된다. 이들 잡은 제품 대기 동작/정보 처리(801) 큐 내에 위치된다. 이러한 큐 내의 각각의 잡은 기다리고 있는 동작 또는 정보를 지시하는 관련 상태, 이 잡에서 수행된 마지막 처리, 잃어버리거나 또는 추가된 정보가 제공되거나, 또는 요구되는 동작이 성공적으로 완료되는 경우 이 잡이 큐잉되는 다음 처리를 갖는다.

소정의 처리의 종료는 작업 흐름 관리자(154)가 이 큐를 체크하고, 이 큐 내의 소정의 잡이 이러한 처리(동작)의 완료 또는 이러한 처리에 의해 제공된 정보를 기다리고 있었는지를 결정한다. 만약 그렇다면, 해당 잡은 적절한 처리 큐에 큐잉된다.

2. 새로운 컨텐츠 요구 처리(802)

컨텐츠 제공자(들)(101)는 그들이 전자적으로 판매 및 전달하고자 하는 제품(예를 들면, 노래 또는 노래의 모음일 수 있는 제품)을 결정한다. 작업 흐름 관리자(154)의 초기 기능은 오퍼레이터를 인에이블시켜 이들 제품을 식별하고, 그룹을 새로운 컨텐츠 요구 처리(802)의 큐 상에 위치시키는 것이다. 컨텐츠 제공자(들)(101)는 구성 옵션을 통해, 어떠한 정보가 제품 선택 인터페이스 상에 프롬프트될지를 특정할 수 있다. 제품을 개별적으로 식별하기 위해 충분한 정보가 입력된다. 선택적으로, 메타데이터 획득과 함께 오디오 처리 상태를 개시하는데 요구되는 정보의 수동 입력을 요구하기 위해 추가적인 필드가 포함될 수 있다. 만약 수동적으로 제공되지 않는다면, 이 정보는 디폴트 구성 설정으로부터 또는 자동 메타데이터 획득 처리(803)에서와 같이 메타데이터 처리의 제 1 단계에서 획득된 컨텐츠 제공자(들)의 데이터베이스(160)로부터 선택적으로 인출될 수 있다. 컨텐츠 제공자(들)의 데이터베이스(113) 내의 컨텐츠(113)의 구성 및 능력이 컨텐츠 선택 처리를 결정한다.

컨텐츠 제공자(들)(101)의 데이터베이스(160)에 대한 요구(query)를 수행하는 데 필요한 원하는 정보가 특정(specify)되면, 잡(job)은 자동 메타데이터 획득 프로세스(803)에 의해 처리된다. 음악 예(music embodiment)에서, 오디오 프로세스를 위한 제품을 적절하게 스케쥴링(schedule)하기 위해, 제품의 장르를 결정하고(genre) 오디오 PCM 또는 WAV 파일 이름(들)과 함께 원하는 압축 레벨이 특정된다. 이 정보는 제품 선택 프로세스의 일부로서 입력(enter)될 수도 있고, 커스텀화된 요구 인터페이스(a customized query interface) 또는 웹 브라우저 기능을 통해 선택될 수도 있다. 이 정보의 특성(specification)을 이용하여 제품이 컨텐츠 프로세스를 위해 스케쥴링될 수 있다.

제품 선택 사용자 인터페이스는 제품이 프로세스를 위해 배포(release)될 지 아니면 보다 많은 정보 진입(entry)을 기다리면서 대기할 지를 조작자(operator)가 특정할 수 있게 하는 선택사양(option)을 제공한다. 대기하는 경우, 프로세스를 위한 제품의 배포 및/또는 데이터 진입의 완료를 위한 이후의 동작을 대기하면서 새로운 컨텐츠 요구 프로세스(802)의 큐에 잡이 추가된다. 제품이 배포되면, 잡 흐름 관리자(154)는 특정된 정보를 평가하고, 잡이 전달(pass)될 프로세스가 어느 것인지를 결정한다.

적절한 정보가 제공되어 컨텐츠 제공자(들)(101)의 데이터베이스(160)에 대한 자동 요구(automated query)를 인에이블시키면, 잡은 자동 메타데이터 획득 프로세스(803)를 위해 큐잉(queue)된다. 데이터 맵핑 테이블이 자동 메타데이터 획득 프로세스(803)를 위해 배열(configured)되지 않았으면, 잡은 수동 메타데이터 진입 프로세스(804)를 위해 큐잉된다(데이터베이스 맵핑 테이블에 관한 세부 사항은 자동 메타데이터 획득 프로세스(803)를 참조).

오디오 프로세스를 위해 필요한 일반 정보 또는 워터마킹을 위해 필요한 특정 정보가 특정되면, 잡은 워터마킹 프로세스(808)(컨텐츠 프로세스의 제 1 단계(phase))를 위해 큐잉된다. 잡이 배포될 때 필요한 정보 중 어느 하나라도 손실(miss)되면, 잡은 정보가 손실되었음을 나타내는 상태(status)와 함께 제품 대기 동작/정보 프로세스(801)의 큐에 큐잉된다.

상태가 컨텐츠(113)의 파일 이름, 예컨대, 컨텐츠(113)가 오디오이고, PCM 또는 WAV 파일이 손실된 경우를 나타내면, 이는 포착(capture)(또는 디지털 매체로부터의 디지털 인출(extraction))이 필요함을 나타낼 수도 있다. 오디오 처리 기능은 노래 파일이 표준 파일 시스템 인터페이스를 통해 엑세스될 것을 요구한다. 노래가 외부 매체 또는 오디오 프로세스 툴이 직접 액세스할 수 없는 파일 시스템 상에 위치하면, 파일은 먼저 엑세스할 수 있는 파일 시스템으로 카피된다. 노래가 CD나 디지털 테이프 상의 디지털 포맷을 취하고 있으면, 이들은 오디오 프로세스 툴에 엑세스할 수 있는 파일 시스템으로 인출된다. 파일을 엑세스할 수 있게 되면, 워터마킹을 위해 필요한 모든 다른 정보가 특정되었다고 가정할 때, 잡 흐름 관리자 사용자 인터페이스(700)는 잡이 워터마킹 프로세스로 배포될 수 있도록 잡을 위한 경로와 파일 이름을 특정하거나 선택하는 데 이용된다.

3. 자동 메타데이터 획득 프로세스(803)

자동화된 방식으로 가능한 한 많은 제품 정보를 수집하려는 시도 중에, 자동 메타데이터 획득 프로세스(803)는 컨텐츠 제공자(들)(101)의 데이터베이스(160) 또는 데이터가 유입(import)되는 단계적(staging) 데이터베이스에 대한 일련의 요구를 수행한다. 자동 메타데이터 획득 프로세스(803)는 항목(items)을 자신의 큐에 저장하기 전에 다음 정보를 요구한다.

· 컨텐츠 제공자(들)(101)의 데이터베이스(160)에 대한 요구를 생성하기 위해 적절한 정보를 구비하는 데이터 맵핑 테이블

· 요구를 수행하는 데 필요한 제품 정보

· 제품을 고유하게 정의하기 위한 적절한 제품 정보

자동화된 요구는 이 컨텐츠(113)를 처리하는 데 필요한 정보를 수집하기 위해, 컨텐츠 제공자(들)(101)의 데이터베이스(160)에 대해 수행된다. 예를 들어, 컨텐츠(113)가 음악이면, 이 요구를 수행하는 데 필요한 정보는 앨범 이름일 수도 있고, UPC 또는 컨텐츠 제공자(들)(101)가 정의한 특정 앨범 또는 선택 ID일 수도 있다. 필요하다면, 수집될 정보 중에서 소정의 것(some)이 지정된다(세부 사항을 위해서는 자동 메타데이터 획득 프로세스(803)에 관한 섹션을 참조). 필요한 모든 데이터가 수집되면, 잡은 사용 조건 프로세스(805)를 위해 다음으로 큐잉된다. 원하는 정보가 손실되면, 노래는 수동 메타데이터 진입 프로세스(804)를 위해 큐잉된다. 제품 대기 동작/정보 프로세스(801) 큐 내의 임의의 잡이 이 단계에서 수집된 임의의 정보를 대기하고 있으면, 잡 상태는 이 정보를 더 이상 대기하지 않음을 나타내도록 갱신된다. 잡이 어떠한 두드러진 조건(outstanding requirements)도 갖지 않으면, 잡은 다음으로 정의된 큐에 큐잉된다.

4. 수동 메타데이터 진입 프로세스(804)

수동 메타데이터 진입 프로세스(804)는 조작자가 손실된 정보를 입력할 수 있는 수단을 제공한다. 어떠한 의존관계(dependencies)도 없다. 원하는 모든 정보가 특정되면, 잡은 사용 조건 프로세스(805)를 위해 큐잉된다.

5. 사용 조건 프로세스(805)

사용 조건 프로세스(805)는 제품 사용 및 제한을 특정한다. 사용 조건 프로세스(805)는 소정의 메타데이터를 필요로 할 수도 있다. 사용 조건 특정이 완료되면, 감독된 배포 프로세스(806) 사양이 요청되거나 잡 흐름 관리자(154) 규칙(rules) 내에서 디폴트(default)로 배열되지 않는 한 잡은 메타데이터 SC(들) 생성 프로세스(807)를 위해 큐잉될 수 있다. 이러한 경우, 잡은 감독된 배포 프로세스(806)를 위해 큐잉된다. 메타데이터 SC(들) 생성 프로세스(807)에 큐잉되기 전에, 잡 흐름 관리자(154)는 먼저 그 프로세스를 위한 모든 의존관계가 만족되었다고 가정한다(아래 참조). 그렇지 않으면, 잡은 제품 대기 동작/정보 프로세스(801)로 큐잉된다.

6. 감독된 배포 프로세스(806)

감독된 배포 프로세스(806)는 디지털 컨텐츠 제품을 위해 특정된 정보의 품질을 체크하고 유효화(validate)한다. 어떠한 의존관계도 없다. 이 제품을 위한 프로세스의 임의의 단계에서 잡에 미리 부착된 커멘트(comments)는 감독자(Supervisor)에 의해 검토되고 적절한 조치가 취해진다. 모든 정보와 커멘트를 검토한 후, 감독자는 다음 선택 사양을 갖게된다.

· 메타데이터 SC(들) 생성 프로세스(807)를 위한 제품의 배포와 큐잉을 승인한다.

· 메타데이터 SC(들) 생성 프로세스(807)를 위해 정보를 수정 및/또는 추가하고 제품을 큐잉한다.

· 잡에 커멘트를 추가하고 수동 메타데이터 진입 프로세스(804)를 위해 제품을 큐잉한다.

· 제품 대기 동작/정보 프로세스(801)를 위해 잡을 큐에 큐잉하고 커멘트를 추가한다.

7. 메타데이터 SC(들) 생성 프로세스(807)

메타데이터 SC(들) 생성 프로세스(807)는 메타데이터 SC(들)(620)를 위해 필요한 다른 정보와 위에서 수

집된 모든 정보를 모으고 SC(를) 포장(packer) 프로세스를 호출하여 메타데이터 SC(를)(620)를 생성한다. 이 툴은 다음을 입력으로 요구한다.

· 필요한 메타데이터

· 사용 조건

· 이 제품의 모든 품질 레벨의 암호화 단계에서 사용된 암호화 키(keys)

이러한 최후의 의존관계는 메타데이터 SC(를)(620)이 생성되기 이전에 관련된 오디오 객체가 오디오 프로세스 단계를 완료할 것을 요구한다. 메타데이터 SC(를) 생성 프로세스(807)가 완료되면, 정의된 잡 흐름 규칙에 기초하여 최종 품질 보증 프로세스(813)나 컨텐츠 보급 프로세스(814)를 위한 큐로 잡이 큐잉된다.

8. 워터마킹 프로세스(808)

워터마킹 프로세스(808)는 컨텐츠(113)에 저작권(copyright)과 기타 정보를 추가한다. 컨텐츠(113)가 노래인 실시예에서, 이 툴은 입력으로서 다음을 요구한다.

· 노래 파일 이름(들)(앨범이 경우 다수 개의 파일 이름)

· 워터마킹 인스트럭션(instructions)

· 워터마킹 파라미터(워터마크에 포함될 정보)

워터마킹 프로세스(808)를 완료하면, 원하는 입력이 이용가능한 경우는 전처리 및 압축 프로세스(809)를 위해 잡이 큐잉되고, 그렇지 않은 경우는 제품 대기 동작/정보 프로세스(801)를 위해 잡이 큐잉된다.

9. 전처리 및 압축 프로세스(809)

전처리 및 압축 프로세스(809)는 임의의 원하는 전처리를 먼저 수행하는 특정한 압축 레벨로 컨텐츠(113)를 부호화(encode)한다. 이 큐에 잡을 큐잉하면 실제로 다수의 큐 엔트리가 생성된다. 원하는 제품의 각 압축 레벨에 따라 잡이 생성된다. 부호화 프로세스는 다수의 시스템 상에서 병렬로 수행될 수 있다. 이 툴은 다음을 입력으로 요구한다.

· 워터마킹된 컨텐츠 파일 이름(들)(컨텐츠(113)가 앨범인 경우 다수 개의 파일 이름)

· (사전배열될 수 있는) 제품 품질 레벨

· (사전배열될 수 있는) 압축 알고리즘

· (전처리기가 필요로 하는 경우) 제품 장르

부호화 프로세스 완료 시, 잡 흐름 규칙에 의해 배열되면 잡은 컨텐츠 품질 제어 프로세스(810)로 큐잉된다. 그렇지 않으면, 잡은 암호화 프로세스(811)로 큐잉된다.

도 11에서는, 부호화 툴의 제 3 제공자가 처리된 오디오와 같은 컨텐츠(113)의 일부(percentage)를 디스플레이하는 방법 또는 선택된 컨텐츠(113)의 전체 선택의 일부로서 부호화된 컨텐츠(113)의 양을 나타내는 방법을 제공하지 않는 경우, 도 8의 컨텐츠 전처리 및 압축 툴을 위한 디지털 컨텐츠의 부호화 레이트(encoding rate)를 결정하는 방법의 흐름도(1100)가 도시되어 있다. 이 방법은 원하는 부호화 알고리즘 및 비트 레이트를 선택하는 단계(1101)로부터 시작된다. 다음으로, 단계(1102)에서는 이 알고리즘과 부호화 레이트가 미리 계산된 레이트 인자(rate factor)를 갖는지를 판단하도록 요구한다. 레이트 인자는 특정한 부호화 알고리즘 및 특정한 비트 레이트에 대한 압축 비율을 결정하는 데 사용되는 인자이다. 미리 계산된 레이트 인자가 저장되지 않았으면, 컨텐츠(113)의 샘플이 사전결정된 회수만큼 부호화된다. 바람직한 실시예에서 사전결정된 시구간은 수 초이다. 사전결정된 시구간에 대한 부호화 레이트는 새로운 레이트 인자 R_{EN}를 계산하는 데 사용된다. 단계(1108)에서 시간의 양과 부호화된 컨텐츠(113)의 양을 알고, 새로운 레이트 인자를 계산하면, R_{EN} = 부호화된 디지털 컨텐츠의 길이 / 시간의 양이다. 단계(1109)에서는 컨텐츠(113)가 부호화되고, 이전에 계산된 레이트 인자를 이용하여 부호화 상태가 디스플레이된다. 이어서, 단계(1107)에서는 이 부호화 알고리즘 및 부호화 비트 레이트를 위해 나중에 사용되기 위해 부호화된 레이트 인자 R_{EN}가 저장된다. 단계(1104)에서는 컨텐츠(113)가 부호화되고, 이전에 계산된 레이트 인자 R_{STORED}를 이용하여 진행 상황(progression)이 디스플레이된다. 한편, 단계(1105)에서는 선택된 알고리즘 및 비트 레이트를 위해 현재 레이트 인자 $R_{CURRENT}$가 계산된다. 단계(1106)에서 현재 레이트 인자 $R_{CURRENT}$는 저장된 레이트 인자를 갱신하는 데 사용되는데, R_{EN} = (R_{STORED} + $R_{CURRENT}$)의 평균이다. 반복해서 레이트 인자를 갱신하면, 특정한 부호화 알고리즘 및 비트 레이트에 대해 매번 점점 더 부호화 레이트를 보다 정밀하게 결정할 수 있다. 단계(1107)에서는 새로운 레이트 R_{EN}가 장래에 사용되기 위해 저장된다. 현재 레이트 인자 $R_{CURRENT}$가 주어진 범위 또는 임계값만큼 사전에 저장된 레이트 인자 R_{STORED}를 벗어나지 않으면 R_{STORED}는 갱신되지 않는다.

이어서, 부호화 상태가 디스플레이된다. 부호화 상태는 현재 부호화 레이트와 함께 컨텐츠(113)에 대한 파일의 전체 길이와 부호화 레이트에 기초하여 진행 상황 바(a progression bar)로서 디스플레이된 전체 컨텐츠(113)의 일부를 포함한다. 부호화 상태는 부호화를 위해 남은 시간도 포함한다. 부호화를 위해 남은 시간은 계산된 부호화 레이트 $R_{CURRENT}$를 컨텐츠(113)에 대한 전체 파일 길이로 나눔으로써 계산된다. 부호화 상태는 호출 프로세스를 호출할 수 있는 다른 프로그램으로 전달될 수 있다. 이는 부호화할 감독 프로그램(supervisory program)이나 부호화할 상호의존(co-dependent) 프로그램이 보다 효율적인 프로세스를 위해 작동하고 일괄처리(batch)하도록 돕는다. 다른 실시예에서는 부호화가 워터마킹 단계를 포함할 수 있다는 사실을 이해해야 한다.

10. 컨텐츠 품질 제어 프로세스(810)

컨텐츠 품질 제어 프로세스(810)는 기능 면에서 감독된 배포 프로세스(806)와 유사하다. 이는 수행되는 컨텐츠 프로세스의 품질을 유효화하는 선택적인 단계이다. 워터마킹 프로세스(808)와 전처리 및 압축 프로세스(809)의 부호화 부분을 제외하고는 의존관계가 없다. 컨텐츠 품질 제어 프로세스(810) 시에는 다음 선택사양을 이용할 수 있다.

·잡은 암호화 프로세스(811)를 위해 배포되고 큐잉될 수 있다.

·커멘트가 추가될 수 있고 하나 이상의 잡이 전처리 및 압축 프로세스(809)를 위해 다시 큐잉될 수 있다.

마지막 선택 사양은 노래 파일의 부호화되지 않은 워터마킹된 버전(version)이 컨텐츠 품질 제어 프로세스(810) 후까지 이용가능할 것을 요구한다.

11. 암호화 프로세스(811)

암호화 프로세스(811)는 워터마킹/부호화된 노래 파일 각각을 암호화하기 위해 적절한 안전한 디지털 컨텐츠 전자 보급 권리 관리 기능을 호출한다. 이 프로세스는 다른 모든 오디오 프로세스의 완료를 제외하고는 의존 관계가 없다. 암호화 프로세스(811)를 완료하면, 잡은 컨텐츠 SC(들) 생성 프로세스(812)를 위해 큐잉된다.

12. 컨텐츠 SC(들) 생성 프로세스(812)

컨텐츠 SC(들) 생성 프로세스(812)는 소정의 메타데이터 파일이 컨텐츠 SC(들)(630)에 포함될 것을 요구한다. 컨텐츠(113) 이외의 파일이 필요한 경우에는 파일이 수집되고, SC(들) 포장 프로세스가 호출되어 생성된 컨텐츠(113)(예컨대, 노래)의 각 압축 레벨에 대해 컨텐츠 SC(들)(630)를 생성한다. 컨텐츠 SC(들) 생성 프로세스(812)를 완료하면, 노래는 정의된 잡 흐름 규칙에 기초하여 최종 품질 보증 프로세스(813) 또는 컨텐츠 보급 프로세스(814) 큐에 큐잉된다.

13. 최종 품질 보증 프로세스(813)

최종 품질 보증 프로세스(813)는 관련된 메타데이터와 컨텐츠 SC(들)(630) 사이의 교차 참조(cross reference)를 체크하여 이들이 올바르게 일치하며 포함된 모든 정보와 컨텐츠(113)가 올바르다는 것을 입증하는 선택적인 단계이다. 최종 품질 보증 프로세스(813)를 완료하면, 컨텐츠 보급 프로세스(814)를 위해 잡이 큐잉된다. 문제가 발견되면, 대부분의 경우 잡은 실패한 단계로 다시 큐잉된다. 이 단계에서 재작업(rework)을 하면, 제품이 문제를 정정하기 위해 필요한 재프로세스(reprocessing)와 함께 재암호화 및 재포장 단계를 거쳐야 하기 때문에 훨씬 비용이 많이 든다. 컨텐츠(113)의 품질과 정보의 정밀도 및 완결성을 보장하기 위해 먼저 보증 단계를 사용할 것을 강력히 추천한다.

14. 컨텐츠 보급 프로세스(814)

컨텐츠 보급 프로세스(814)는 SC(들)을 적절한 호스팅 싸이트(hosting sites)로 전달하는 역할을 한다. 성공적으로 SC(들)을 전달한 후, 잡 완료 상태가 로깅(log)되고, 잡은 큐로부터 삭제된다. SC(들)을 전달하는 중에 문제가 발생하면, 정의된 회수만큼 재시도한 후, 잡은 에러가 발생하여 실패한 것으로 잡 흐름 관리자 툴(154)에 플래그(flag)된다.

15. 잡 흐름 규칙

도 8에 대한 잡 흐름 규칙은 다음과 같이 3 개의 주된 시스템에서 동작한다.

A : 잡 흐름 관리자 툴(154)

1. 새로운 컨텐츠 요청 프로세스(802)

2. 제품 대기 동작/정보 프로세스(801)

3. 최종 품질 보증 프로세스(813)

4. 컨텐츠 보급(및 통지) 프로세스(814)

B : 메타데이터 동화(assimilation) 및 진입 툴(161)

1. 자동 메타데이터 획득 프로세스(803)

2. 수동 메타데이터 진입 프로세스(804)

3. 감독된 배포 프로세스(806)

4. 메타데이터 SC(들) 생성 프로세스(807)

C : 컨텐츠 처리 툴(155)

1. 워터마킹 프로세스(808)(저작권 데이터를 필요로 함)

2. 전처리 및 압축 프로세스(809)

3. 컨텐츠 품질 제어 프로세스(810)

4. 암호화 프로세스(811)

5. 컨텐츠 SC(들) 생성 프로세스(812)

작업 흐름

컨텐츠(113) 선택 조작자는 새로운 제품을 입력하고 A1(새로운 컨텐츠 요청 프로세스(802)) 상으로의 큐잉을 개시한다.

A1 : 컨텐츠(113) 선택 조작자가 이를 작업 흐름 관리자 툴(154)로 배포하면, B1(자동 메타데이터 획득 프로세스(803)) 상으로 큐잉된다.

A2 : B4(메타데이터 SC(들) 생성 프로세스(807))로 이어지는 단계 B1(자동 메타데이터 획득 프로세스(803))나, 단계 B2(수동 메타데이터 진입 프로세스(804))나, 단계 B3(감독된 배포 프로세스(806))으로부터 옴[암호화 키를 필요로 함].

단계 A3(최종 품질 보증 프로세스(813))이나 단계 A4(컨텐츠 보급 프로세스(814))로 이어지는 B4(메타데이터 SC(들) 생성 프로세스(807))로부터 옴[컨텐츠 SC(들)(630)을 필요로 함].

단계 C2(전처리 및 압축 프로세스(809))로 이어지는 단계 C1(워터마킹 프로세스(808))로부터 옴[전처리 및 압축 프로세스(809)를 위해 메타데이터를 필요로 함].

단계 C5(컨텐츠 SC(들) 생성 프로세스(812))로 이어지는 단계 C4(암호화 프로세스(811))로부터 옴[컨텐츠 SC(들)(630) 포장을 위해 메타데이터를 필요로 함].

단계 A3(최종 품질 보증 프로세스(813))나 단계 A4(컨텐츠 보급 프로세스(814))로 이어지는 단계 C5(컨텐츠 SC(들) 생성 프로세스(812))로부터 옴[메타데이터 SC(들)(620)을 필요로 함].

A3 : 단계 A3(최종 품질 보증 프로세스(813)) 후에, 큐 B2(수동 메타데이터 진입 프로세스(804)) 상에 배치하거나, 큐 B3(감독된 배포 프로세스(806)) 상에 배치하거나, 품질 보증 조작자가 필요로 하는 큐에 배치한다.

A4 : 단계 A4(컨텐츠 보급 프로세스(814)) 후에, 잡 흐름 관리자 툴(154)이 이 제품을 위해 수행된다.

B1 : 단계 B1(자동 메타데이터 획득 프로세스(803)) 후에, 단계 C1(워터마킹 프로세스(808))를 위해 필요한 메타데이터가 존재하면, 이 제품을 나타내는 엔트리를 큐 C1 상에 배치한다.

(다음 로직도 수행)

하나 또는 2 개의 임의의 필요한 메타데이터가 손실된 경우, 수동 메타데이터 제공자로의 커멘트가 존재하면, 큐 B2(수동 메타데이터 진입 프로세스(804)) 상에 제품을 배치하고,

이 제품에 대해 감독된 배포가 요청되면, 큐 B3(감독된 배포 프로세스(806)) 상에 제품을 배치하며,

제품이 요청된 품질 레벨 모두에 대해 컨텐츠 처리 툴(155)로부터의 모든 정보를 가지면, 큐 B4(메타데이터 SC(들) 생성 프로세스(807)) 상에 제품을 배치하고,

그렇지 않으면, 제품을 암호화 키로서 플래그하고 큐 A2(제품 대기 동작/ 및 정보 프로세스(801)) 상에 제품을 배치한다.

B2 : 단계 B2 동안(수동 메타데이터 진입 프로세스(804)),

단계(C1)(워터마킹 프로세스(808))가 행해지지 않고, 단계(C1)에 필요한 메타데이터가 존재하면, 이러한 제품을 나타내는 엔트리를 대기 행렬(C1) 상에 배치 (또한, 다음 논리 동작을 수행).

단계(C2)(전처리와 압축 프로세스(809))에 필요한 메타데이터가 바로 제공되었다면,

(또한, 다음 논리 동작을 수행)

메타데이터 등화 및 진입 툴(161)에 의해 수집될 수 있는 메타데이터가 존재하면,

그러하다면,

이러한 제품에 대해 감독된 배포가 요구되었다면, 제품을 대기 행렬(B3) 상에 배치 (감독된 배포 프로세스(806))

그렇지 않다면,

컨텐츠 선처리 툴(155)의 단계(C4)(암호화 프로세스(811))로부터의 정보 모두가 존재하면, 이러한 제품을 대기 행렬(Before) 상에 배치 (메타데이터 SC 생성 프로세스(807))

그렇지 않다면, 암호화 키를 필요로 할 때 제품을 플래그하고 이 제품을 대기 행렬(A2) 상에 배치 (제품 대기 동작/정보 프로세스(801)).

그렇지 않다면,

메타데이터 제공자가 강제 감독 배포(a forced supervised release)를 요구하였다면, 이 제품을 대기 행렬(B3) 상에 배치 (감독된 배포 프로세스(806))

그렇지 않다면, 미실행 (제품을 대기 행렬(B2)상에 유지 (수동 메타데이터 진입 프로세스(804)))

B3 : 단계(B3) 동안(감독된 배포 프로세스(806))

조작자가 역으로 단계(B2)에 제품을 보내고 있다면 (수동 메타데이터 진입 프로세스(804)), 제품을 대기 행렬(B2) 상에 배치.

그렇지 않고, 조작자가 제품을 배포하였다면,

컨텐츠 처리 툴(155)의 단계(C4)(암호화 처리(811))로부터의 정보 모두가 존재하다면,

이 제품을 대기 행렬(Before) 상에 배치 (메타데이터 SC 생성 프로세스)

그렇지 않다면, 암호화 키를 필요로 할 때 제품을 플래그하고 이 제품을 대기 행렬(A2) 상에 배치 (제품 대기 동작/정보 프로세스(801)).

그렇지 않다면, 제품은 대기 행렬(B3) 상에 잔존 (감독된 배포 프로세스(806)).

Before : 단계(Before) 후 (메타데이터 SC 생성 프로세스(807)),

팩킹된 제품 메타데이터를 플래그.

(제품/품질 레벨) 튜플 모두가 압축되었다면,

컨텐츠 제공자(101)의 환경 설정이 SC의 품질 보증을 지정하고 있다면, 이 제품을 대기 행렬(A3) 상에 배치 (최종 품질 보증 처리(813))

그렇지 않다면, 이 제품을 대기 행렬(A4) 상에 배치 (컨텐츠 보급 프로세스(814)).

그렇지 않다면, SC의 컨텐츠(113)를 필요로 할 때 제품을 플래그하고 제품을 대기 행렬(A2) 상에 배치 (제품 대기 동작/정보 프로세스(801)).

C1 : 단계(C1) 후 (워터마킹 프로세스(808)),

단계(C2)(전처리 및 압축 프로세스(809))에 필요한 메타데이터가 존재한다면, 각각의 (제품/품질 레벨) 튜플에 대한 엔트리를 생성하고 대기 행렬(C2) 상에 배치.

그렇지 않다면, 전처리/압축을 위해 메타데이터를 필요로 할 때 제품을 플래그하고 이 제품을 대기 행렬(A2) 상에 배치 (제품 대기 동작/정보 프로세스(801)).

C2 : 단계(C2) 후 (전처리 및 압축 프로세스(809)),

컨텐츠 제공자(101)의 환경 설정이 컨텐츠 품질 제어 프로세스(810)를 지정한다면, 이 (제품/품질 레벨) 튜플을 대기 행렬(C3) 상에 배치 (컨텐츠 품질 제어 프로세스(810)),

그렇지 않다면, 이 (제품/품질 레벨) 튜플을 대기 행렬(C4) 상에 배치 (암호화 프로세스(811)).

C3 : 단계(C3) 후 (컨텐츠 품질 제어 프로세스(810)), 이 (제품/품질 레벨) 튜플을 대기 행렬(C4) 상에 배치 (암호화 프로세스(811)).

C4 : 단계(C4) 후 (암호화 프로세스(811)),

필요한 정보(즉, 본 프로세스에 의해 생성되고, 컨텐츠(113)를 암호화하는데 사용되는 대칭 키(623))를 메타데이터 동화 및 진입 툴(161)에 제공.

컨텐츠 SC(630) 팩킹에 필요한 메타데이터 모두가 존재한다면, 이 (제품/품질 레벨) 튜플을 대기 행렬(C5) 상에 배치 (컨텐츠 SC 생성 프로세스(812)).

그렇지 않다면, 컨텐츠 SC(630) 팩킹을 위해 메타데이터를 필요로 할 때 제품을 플래그하고 이 (제품/품질 레벨) 튜플을 A2 상에 배치 (제품 대기 동작/정보 프로세스(801)).

C5 : 단계(C5) 후 (컨텐츠 SC 생성 프로세스(812)),

이러한 품질 레벨에서 컨텐츠(113)가 팩킹된 품질 레벨을 플래그.

(제품/품질 레벨) 튜플 모두가 팩킹되었다면,

메타데이터가 팩킹된 제품이 플래그되면,

컨텐츠 제공자(101)의 환경 설정이 SC의 품질 보증을 지정하면, 이 제품을 대기 행렬(A3) 상에 배치 (최종 품질 보증 프로세스(813))

그렇지 않다면, 이 제품을 대기 행렬(A4) 상에 배치 (컨텐츠 보급 프로세스(814))

그렇지 않다면, 메타데이터 SC(620)를 필요로 할 때 제품을 플래그하고 이 제품을 대기 행렬(A2) 상에 배치 (제품 대기 동작/정보 프로세스(801)).

그렇지 않다면, (모든 (제품/품질 레벨) 튜플이 미팩킹) 미실행 (다른 (제품/품질 레벨) 튜플은 동작을 트리거).

C. 메타데이터 동화 및 진입 툴

메타데이터는 컨텐츠(113), 예를 들어 음악에서의 레코딩의 타이틀, 가수, 작사가/작곡가, 프로듀서 및 레코딩의 길이를 나타내는 데이터로 구성되어 있다. 다음의 설명은 음악이 되는 컨텐츠(113)를 근거로 하고 있지만, 당업자는 다른 컨텐츠 형태, 예를 들어, 비디오, 프로그램, 멀티미디어, 영화 등이 본 발명의 사상과 범위 내에 있다는 것을 알아야 한다.

이 서브시스템에 의해, 컨텐츠 제공자(101)가 전자 디지털 컨텐츠 상점(103)에 제공하는 데이터, 컨텐츠 제공자(101)가 엔드 유저에게 구매 제품과 함께 제공하는 데이터, 및 컨텐츠 제공자(101)가 엔드 유저에게 제공하고자 하는 다른 구매 옵션(사용 조건(517))은 제품(예를 들어, 음악에서, 가수의 샘플 클립, 가수의 히스토리, 이 레코딩이 나타내는 앨범의 리스트, 가수 및/또는 제품과 연관된 장르)의 판매를 판촉하는데 도움이 된다. 데이터는 전자 디지털 컨텐츠 상점(103)에서 이용가능한 메타데이터 SC(620)으로 팩킹된다. 목적 달성을 위해, 다음의 툴이 제공된다.

자동 메타데이터 획득 툴

수동 메타데이터 진입 툴

사용 조건 툴

감독된 배포 툴

이러한 툴을 이용하여 컨텐츠 제공자(101)는 작업 흐름 관리자(154)에 대한 상술한 프로세스를 구현할 수 있다. 바람직한 실시예에서 툴은 자바(Java) 계통의 툴키트이지만, C/C++, 어셈블러 등과 같은 다른 프로그래밍 언어가 사용될 수 있다.

1. 자동 메타데이터 획득 툴

자동 메타데이터 획득 툴을 이용하여 유저는 상술한 자동 메타데이터 획득 프로세스(803)를 구현할 수 있다. 자동 메타데이터 획득 툴은 컨텐츠 제공자(101)의 메타데이터에 액세스하는데 사용되고, 오퍼레이터의 도움없이 가능한 한 많은 양의 데이터를 검색하는데 사용된다. 환경 설정 방법은 이러한 프로세스를 자동화하는데 이용가능하다. 컨텐츠 제공자(101)는 자신이 엔드 유저에게 제공하기를 원하는 데이터 유형(예를 들어, 작곡가, 프로듀서, 연주자, 트랙 길이)과, 전자 디지털 컨텐츠 상점(103)에 제공하는 판촉 데이터 유형(음악을 예를 들어, 가수에 의한 샘플 클립, 가수의 히스토리, 레코딩이 나타내는 앨범의 리스트, 가수와 연관된 장르)을 확인하기 위해 디폴트 메타데이터 템플릿을 변경할 수 있다. 디폴트 메타데이터 템플릿은 엔드 유저 장치(109)가 필요로 하는 데이터 필드, 엔드 유저 장치(109)에 옵션적으로 제공될 수 있는 데이터 필드 및 전자 디지털 컨텐츠 상점을 목표로 하여 가수, 앨범, 및/또는 싱글을 판촉하는 데이터 필드의 샘플 세트를 포함하고 있다.

컨텐츠 제공자(101)의 데이터베이스(160)로부터 템플릿 데이터 필드를 인출하기 위해서, 자동 메타데이터 획득 툴은 데이터를 찾을 수 있는 데이터베이스 내의 위치에 데이터 유형(예, 작곡가, 프로듀서, 가수의 일대기)을 매핑하는 테이블을 이용한다. 컨텐츠 제공자(101) 각각은 그들의 환경에 맞게 그 매핑 테이블을 지정하는 것을 도와준다.

자동 메타데이터 획득 툴은 컨텐츠 제공자(101)의 데이터베이스(160)로부터 이용가능한 어떠한 데이터도 획득하기 위해서, 컨텐츠 제공자(101)의 메타데이터 템플릿과 매핑 테이블을 이용한다. 각 제품의 상태는 자동 메타데이터 획득 프로세스(803)의 결과에 따라 갱신된다. 임의의 획득 데이터를 누락한 제품은 수동 메타데이터 진입 프로세스(804)를 위해 대기되고, 그렇지 않으면, 메타데이터 SC(620)로 팩킹하기 위해 이용가능하다.

2. 수동 메타데이터 진입 툴

수동 메타데이터 진입 툴을 이용하여, 사용자는 상술한 수동 메타데이터 진입 프로세스(804)를 실행할 수 있다. 수동 메타데이터 진입 툴에 의해, 적당히 인증된 오퍼레이터는 누락 데이터를 제공할 수 있다. 오퍼레이터가 누락 데이터가 이용불가능하다고 판단하면, 오퍼레이터는 제품에 코멘트를 달고, 감독된 배포를 요구한다. 컨텐츠 제공자(101)는 품질 보증을 이유로, 제품이 감독된 배포에 영향을 주어야 함을 요구할 수 있다. 일단 모든 요구된 데이터가 존재하면, 감독된 배포가 요구되지 않았을 경우에, 제품은 메타데이터 SC(620)로 팩킹하기 위해 이용가능하다.

3. 이용 조건 툴

이용 조건 툴을 이용하여, 사용자는 상술한 이용 조건 프로세스(805)를 실행시킬 수 있다. 전자 배송(electronic delivery)을 이용한 판매 또는 대여(사용 제한)용 컨텐츠(113)를 제공하는 프로세스는 일련의 비지니스 결정과 연관되어 있다. 컨텐츠 제공자(101)는 컨텐츠(113)이 이용가능한 압축 레벨을 결정한다. 그 다음, 각각의 압축된 인코딩 버전의 컨텐츠(113)에 대하여, 하나이상의 이용 조건이 명시된다. 각각의 이용 조건은 컨텐츠(113)의 이용에 관하여, 엔드 유저의 권리 및 엔드 유저의 이용 제한을 정의한다.

컨텐츠 처리 툴(155)의 부품으로서, 이용 조건 세트(엔드 유저 권리와 이용제한)는 제품에 부착된다.

이용 조건은 다음을 정의하고 있다.

1. 이러한 이용 조건이 적용되는 압축 인코딩 버전의 컨텐츠(113).

2. 이러한 이용 조건에 의해 커버되는 유저의 유형(예를 들어, 비지니스, 개인 소비자).

3. 이러한 이용 조건에 의한 컨텐츠(113)의 구매 또는 대여 가능 여부.

   대여 거래에 대하여

   - 대여 기간을 제한하는데 사용되는 치수 단위.
   - 컨텐츠(113)가 더 이상 재생하지 않을 치수 단위의 수.

   구매 거래에 대하여

   - 엔드 유저가 만들 수 있는 재생 가능 카피본의 수.
   - 이러한 카피본을 만들 수 있는 미디어의 종류(예를 들어, CD-R, 미니디스크, 퍼스널 컴퓨터).

4. 구매/대여 거래가 일어날 수 있는 시간(즉, 엔드 유저가 초기 이용가능 날짜 후와 최종 이용가능 날짜 전에만 이러한 이용 조건 기간중에 구매/대여할 수 있다).

5. 엔드 유저가 이러한 구매(또는 대여)를 거래할 수 있는 나라.

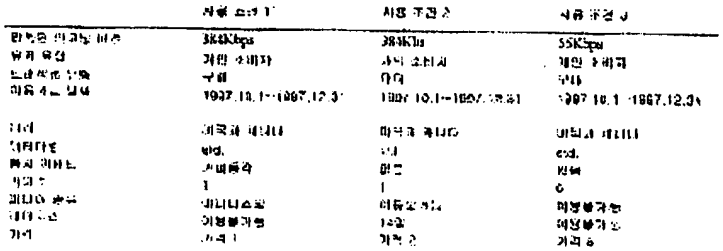
6. 이러한 이용 조건하에서의 구매/대여 거래의 가격.

7. 워터마킹 파라미터.

8. 결재소의 통지서를 요구하는 이벤트의 유형.

이용 조건 세트의 예

컨텐츠 제공자(101)는 1997년 4분기동안 인기있는 어린 보컬리스트가 부른 동요의 재배포를 받아드린 북아메리카 시장을 테스트하기로 결정할 것이다. 테스트는 두 개의 상이한 압축 인코딩 버전, 384Kbps와 56Kbps으로 이용가능한 노래를 만들 것이다. 384Kbps 버전은 판매될 수 있거나(미니디스크에 만들어진 하나의 카피본), 또는 (2주동안) 대여될 수 있지만, 56Kbps 버전은 판매만 가능하다(만들어진 카피본이 없다). 워터마킹 명령은 구매/대여와 동일하고, 컨텐츠 제공자(101)는 결재소(105)가 모든 만들어진 카피본을 계산하기를 원한다. 이로 인해 다음과 같은 이용 조건이 만들어질 수 있다.



4. 메타데이터 SC(620)의 일부

메타데이터 동화 및 진입 툴(161)이 메타데이터 SC(620)에 포함시키기 위해 모은 일부 데이터 종류가 아래에 있다. 기능과 수신지에 의해 데이터를 SC 부분으로 그룹화하려고 노력하였다.

제품 ID [src:컨텐츠 제공자;]
[dest:모든 사람]
라이센서 라벨 컴파니 [dest:EMS:엔드 유저]
라이센서 라벨 컴파니 [dest:EMS:엔드 유저]
객체(서브라이센스 라벨 컴파니)의 소스(발행자) [dest:모든 사람]
객체의 유형(즉, 단일 객체 또는 객체 어레이)
객체 ID [dest:모든 사람]
국제 표준 레코딩 코드(ISRC)
국제 표준 뮤직 넘버(ISMN)
이용 조건 (src:컨텐츠 제공자;dest:EMS, 엔드 유저, 결재소(105))
구매 이용 조건 (src:EMS; dest:엔드 유저, 결재소(105))
객체 이용에 대한 이용 조건 세트(소비자 이용 제한 및 권리)
(사운드 레코딩)
이용 조건 어레이 내의 개별 엔트리
이러한 이용 조건이 적용하는 컨텐츠(113)의 압축 인코딩 버전
이러한 이용 조건에 의해 컨텐츠(113)의 구매 또는 임대 가능 여부
임대 거래에 있어서,
임대 기간을 제한하는데 사용되는 치수 단위(예, 날짜, 플레이)
컨텐츠(113)가 더 이상 플레이하지 않을 치수 단위수
구매 거래에 있어서,
엔드 유저가 만들 수 있는 재생가능 카피본의 수
이러한 카피본을 만들 수 있는 미디어의 종류(예, CD-R, 미니 디스크, 퍼스널 컴퓨터)
구매/임대 거래가 일어나는 시간
(즉, 초기 이용가능 날짜 후와 최종 이용가능 날짜전에만 이용 조건 기간중에 엔드 유저가 구매/임대할 수 있다)
엔드 유저가 이러한 구매(또는 임대)를 거래할 수 있는 나라에서의 포인터
이러한 이용 조건하의 구매/임대 거래의 가격

암호화된 워터마킹 명령과 파라미터에서의 포인터
결재소(105)의 통지서를 요구하는 이벤트 유형에서의 포인터
구매 데이터 (암호화:옵션 정보:src:EMS:dest:엔드 유저,결재소(105))
구매 날짜
구매 가격
성명 및 주소의 청구서
소비자 성명 및 주소
소비자의 나라(최적 추측)
메타데이터 1 (src:컨텐츠 제공자; dest:EMS, 엔드 유저)
배열{
저작권 정보
작곡에 대한
사운드 레코딩에 대한
노래의 제목
작사가
}
포인터{
삽화(예, 앨범 커버);
삽화의 포맷(예, GIF, JPEG);
}
옵션 정보:
추가 정보 배열{
작곡가
발행자
프로듀서
연주자
레코딩 날짜
배포 날짜
노래
트랙명(기재사항)/트랙 길이
이 레코딩이 나타나는 앨범의 리스트
장르
}
메타데이터 2 (src: 컨텐츠 제공자; dest:EMS)
각각이 동일 사운드 레코딩의 상이한 품질 레벨을 나타내는 구조의 배열
{
사운드 레코딩;
사운드 레코딩의 품질 레벨
(바람직하게 압축된) 사운드 레코딩의 사이즈(바이트 단위)
}
메타데이터 3 (src: 컨텐츠 제공자; dest:EMS, 엔드 유저)
옵션 정보:
판촉 재료:
아티스트 판촉 재료에 대한 포인터{
아티스트 웹 사이트에 대한 URL;

아티스트(들)의 배경 설명(들);

아티스트 관련 인터뷰(인터뷰(예컨대, 텍스트, 오디오, 비디오) 포맷과 함께);

재검토(재검토(예컨대, 텍스트, 오디오, 비디오) 포맷과 함께);

샘플 크립들(이것의 포맷과 압축 레벨);

최근 및 다가오는 콘서트/좀석/이벤트-그들의 날짜 및 위치;

}

앨범 판촉 재료에 대한 포인터(

샘플 클립(이것의 포맷과 압축 레벨);

프로듀서, 및/또는 작곡자, 및/또는 영화/연극/캐스트(cast), 및/또는 앨범 제작 등의 배경 설명(들);

비아티스트 관련 인터뷰(인터뷰(예컨대, 텍스트, 오디오, 비디오) 포맷과 함께);

재검토(재검토(예컨대, 텍스트, 오디오, 비디오) 포맷과 함께);

장르(들);

}

단일 판촉

샘플 클립(이것의 포맷과 압축 레벨);

프로듀서, 및/또는 작곡가, 및/또는 영화/연극/캐스트, 및/또는 싱글(single) 제작 등의 배경 설명(들)

재검토(재검토(예컨대, 텍스트, 오디오, 비디오) 포맷과 함께)

5. 감독된 발매 툴(Supervised Release Tool)

감독된 발매 툴은 전술된 것처럼 감독된 발매 프로세서(806)를 실행할 능력을 유저에게 제공한다. 컨텐츠 제공자(들)(101)이 지시하며 감독된 발매 권한을 갖는 개인은 감독된 발매(즉, 감독된 발매 프로세스(806) 큐상의 제품)를 기다리는 제품을 호출하여, 이것의 컨텐츠(113) 및 수반하는 주석을 조사할 수 있으며,

이것의 컨텐츠(113)를 승인하여, 메타데이터(SC)(620) 내로 패킹하는 제품을 발매하며, 또는

소정의 필요한 정정을 하여 메타데이터(SC)(620) 내로 패킹하는 제품을 발매하며, 또는

교정 동작을 지시하는 주석을 부가하여 이 제품을 매뉴얼 메타데이터 진입 프로세스(704)로 가져가서 다시 제출한다.

또다른 실시예에서, SC(들)를 생성한 후에, SC의 컨텐츠(113)가 완성도와 정밀도에 대해 개방되어 조사될 수 있으며, 그때에 소매 채널로의 제품 발매에 대해 최종 승인되거나 또는 거부될 수 있는 또다른 선택 품질 보증 단계가 존재한다.

0. 컨텐츠 프로세싱 툴

컨텐츠 프로세싱 툴(155)은 워터마크된(watermarked), 인코딩된, 및 암호화된 콘텐츠 사본을 생성하기 위해서 디지털 컨텐츠 파일을 프로세싱하는데 이용되는 소프트웨어 툴들의 집합체다. 이 툴은 디지털 컨텐츠 프로세싱 툴의 산업 표준을 이용하여 그들이 전개하는 워터마킹, 인코딩 및 암호화 기술을 플러거(plug) 가능한 대체를 허락한다. 선택된 산업 툴이 명령 라인 시스템 호출 인터페이스 및 전달된 매개변수를 통해 로딩되거나 DLL 인터페이스를 통해 함수를 호출할 수 있는 툴킷(toolkit)을 제공하는 경우, 컨텐츠 프로세싱은 어느 정도 자동화될 수 있다. 각 툴에 대한 프런트 엔드 애플리케이션은 다음 이용 가능한 일에 대한 컨텐츠 프로세싱 툴(155)에서 적당한 큐에 질문하여, 요구되는 파일들 및 매개변수들을 검색한 다음, 요구된 함수를 수행하기 위해서 산업 표준 컨텐츠 프로세싱 툴을 로딩한다. 이 일을 완성하자 마자, 툴이 종료 상태를 보고하지 않는 경우 큐에 대한 수동 갱신이 요구될 수 있다.

컨텐츠 프로세싱 툴(155)의 포괄적인 버전이 기술되지만, 커스터마이제이션은 가능하다. 컨텐츠 프로세싱 툴(155)은 Java, C/C++ 또는 소정의 장비 소프트웨어로 기록될 수 있다. 컨텐츠 프로세싱 툴(155)은 디스켓, CDS를 포함하는 임의의 컴퓨터 판독 가능한 수단에 의해 또는 웹 사이트를 통해 전달될 수 있다.

1. 워터마킹 툴

워터마킹 툴은 전술된 것처럼 워터마킹 프로세스(808)를 실행할 능력을 유저에게 제공한다. 이 툴은 컨텐츠 (113) 소유자의 판권 정보를 오디오 워터마킹 기술을 이용하는 노래 파일에 인가한다. 기록될 실제 정보는 컨텐츠 제공자(101) 및 선택된 특정 워터마킹 기술에 의해 결정된다. 이 정보는 프런트 엔드 워터마킹 툴에 이용될 수 있으므로, 이 정보를 워터마킹 함수로 적절히 전달할 수 있다. 이것은 융기화 요구를 메타데이터 등화 및 진입 툴(161)에 강제하며, 예컨대 오디오 파일의 노래를 프로세싱하기에 앞서 이 정보를 획득하게 한다. 이 노래는 워터마킹 정보가 획득될 시 까지 오디오 프로세싱에 대해 이용될 수 없다.

워터마크는 생성된 노래의 모든 인코딩들에 공통이기 때문에 오디오 프로세싱에서 제 1 단계로서 인가된다. 워터마크가 인코딩 기술로 견딜 수 있는 한, 워터마킹 프로세스는 노래 당 단지 한번 발생하는 것을 필요로 한다.

다양한 워터마킹 기술들이 공지되고 상업적으로 이용되고 있다. 프런트 엔드 워터마킹 툴은 다양한 산업

워터마킹 툴들을 지원할 수 있다.

2. 프로세싱 및 압축 툴

프로세싱 및 압축 툴은 전술된 것처럼 프로세싱 및 압축 프로세스(809)를 수행할 능력을 유저에게 제공한다. 오디오 인코딩은 2개의 프로세스를 포함한다. 인코딩은 기본적으로 음악 컨텐츠에 대한 예의 경우에, PCM 오디오 스트림에 대한 로시(lossy) 압축 알고리즘의 애플리케이션이다. 인코더는 요구되는 오디오 품질 레벨에 기초한 다양한 재생 비트 스트림 속도를 발생시키도록 조정될 수 있다. 보다 높은 품질은 보다 큰 파일 크기를 야기하고, 이 파일 크기는 고품질 컨텐츠(113)에 대해 매우 크기 때문에, 고품질 컨텐츠(113)용 다운로드 시간은 길어서 때때로 표준 28,800 bps 모뎀들에 대해서는 금지될 수 있다.

따라서, 컨텐츠 제공자(들)(101)은 다운로드 동안 여러 시간 기다리기를 원하지 않는 성급한 저 대역폭 고객들 및 고품질 컨텐츠(113)를 사거나 또는 보다 고속으로 접속하는 오디오광 또는 높은 대역폭 고객들을 달래기 위해서 다양한 다운로드용 디지털 컨텐츠 품질을 제공할 수 있다.

압축 알고리즘은 그들의 기술을 변화시켜, 보다 낮은 속도로 컨텐츠(113)를 재생한다. 이 기술은 알고리즘(즉, MPEG, AC3, ATRAC) 및 압축 레벨에 의해 변한다. 보다 높은 압축 레벨를 이루기 위해서, 데이터는 통상 압축 알고리즘으로 전달되기 전에 보다 낮은 샘플링 속도로 재샘플링된다. 저 손실의 충실도를 갖는 압축을 보다 효율적으로 하거나 또는 임의의 주파수 범위에 대한 철저한 배제를 방지하기 위해서, 디지털 컨텐츠는 때때로 특정 주파수의 융화 레벨에 대한 조정 또는 기록 역학에 대한 조정을 필요로 할 수 있다. 컨텐츠 프로세싱 요구들은 압축 알고리즘 및 요구되는 압축 레벨과 직접적으로 관련이 있다. 몇몇 경우에, 컨텐츠(113)(예컨대, 음악 장르) 유형은 동일한 장르로부터의 노래들이 유사한 역학적 원리를 갖기 때문에 프로세싱 요구들을 결정하는 기초로서 성공적으로 이용될 수 있다. 이들 프로프로세싱(preprocessing) 함수들은 몇몇 압축 툴들과 함께 인코딩 프로세스의 일부이다. 원하는 전처리는 다른 것들과 함께 압축 전에 수행된다.

각각의 노래는 판매용 다운로드 가능한 오디오 파일 외에, 낮은 비트 속도(LBR)로 인코딩된 클립(clip)을 가져서, 노래가 LBR 스트리밍 프로토콜을 통해 샘플링되게 한다. 이러한 LBR 인코딩은 컨텐츠 프로세싱 툴(155)이 책임진다. 이러한 클립은 개별적인 PCM 파일로서 또는 오프셋 및 길이 매개변수들로서 컨텐츠 제공자(들)(101)에 의해 제공된다.

워터마킹에 관해서 처럼, 인코딩 툴은 API 또는 명령 라인 시스템 호출 인터페이스를 통해 로딩될 수 있으며, 전처리 및 압축에 대해 요구되는 매개변수들 모두를 전달한다. 프런트 엔드 인코딩 툴은, 예컨대 컨텐츠가 음악인 경우, 및 소정의 오디오 전처리하기에 앞서 컨텐츠 제공자(툴)의 데이터베이스(16)로부터 노래 장르가 획득되도록 결정되는 경우, 메타데이터 동화 및 진입 툴(161)을 갖는 등기화 요구들을 가질 수 있다. 이것은 선택된 인코딩 툴 및 노래 장르의 불확실한 정도에 의존한다. 컨텐츠 제공자(들)이 노래 당 인코딩되는 품질 레벨에 대한 선택을 변화시키는 경우, 이 정보는 인코딩 단계에 앞서 제공되며, 메타데이터 동화 및 진입 툴(161)이 생성하는 메타데이터와 일치한다.

다양한 고품질 인코딩 알고리즘 및 툴들이 오늘날 공지된다. 프런트 엔드 인코딩 툴은 다양한 산업 인코딩 툴들을 지원할 수 있다.

본 발명에 따른 도 8의 자동 메타데이터 획득 툴에 대한 일 실시예의 순서도가 도 12에 도시된다. 이 프로세스는 컨텐츠 제공자(툴)(101)이 조사하고 있는 매체로부터 식별기를 판독함으로서 시작한다. 오디오 CD 실시예에서 컨텐츠의 일예. 오디오 CD 실시예에서, 아래 코드들은 이용 가능한 유니버설 가격 코드(UPC), 국제 표준 기록 코드(ISRC), 국제 표준 음악 번호(ISMN)다. 이 식별기는 이 컨텐츠에 적합한 플레이어, 예컨대 오디오 CD용 오디오 CD 플레이어, DVD 영화용 DVD 플레이어, DAT 기록용 DAT 기록기 및 등가물에서 판독된다, 단계(1201). 다음에, 이 식별기는 컨텐츠 제공자(툴)(101)용 데이터베이스(160)에 색인을 다는데 이용된다, 단계(1202). 도 8에 기술된 것처럼, 작업 흐름 관리자 프로세스가 요구하는 정보의 일부 또는 모두가 데이터베이스(160) 및 소정의 다른 관련 소스들에서 검색된다, 단계(1203). 이 정보는 컨텐츠(113) 및 이것과 관련있는 메타데이터를 포함할 수 있다. 단계(1204)에서, 검색된 부가적인 정보는 전자 컨텐츠(113)를 생성하는 작업 흐름 관리자(154)를 시작시키는데 이용된다. 여러 개의 오디오 CDS와 같은 여러 미디어 선택물들은 전자 배포용 일련의 컨텐츠(113)를 생성하기 위해서 자동 메타데이터 획득 툴을 인에이블하도록 큐업(queue up)될 수 있다. 예를 들면, 모든 컨텐츠(113)는 일련의 CDS로부터 생성되거나 또는 컨텐츠 제공자(들)(101)가 조사한 하나 이상의 CDS들로부터 선택된 트랙일 수 있다.

이와 다른 실시예에서, 전처리 매개변수들은 컨텐츠 제공자(들)의 데이터베이스로부터 자동으로 검색될 수 있다. 도 13은 전처리 및 전처리의 압축 매개변수들 및 본 발명에 따른 도 8의 압축 툴을 자동으로 설정하는 방법에 대한 순서도다. 이 실시예에서, 컨텐츠(113)는 음악이다. 단계(1301)에서, 음악(컨텐츠(113))은 컨텐츠 프로세싱 툴(155)에서 인코딩되도록 선택된다. 선택된 음악 장르가 결정된다, 단계(1302). 이것은 수동으로 등록되거나 또는 도 12에 기술된 프로세스로부터 검색된 부가적인 데이터와 같은 다른 이용 가능한 메타데이터를 이용하여 등록될 수 있다. 오디오 압축 레벨 및 선택된 오디오 압축 알고리즘이 검사된다, 단계(1303). 다음에, 압축 매개변수들이 전처리 및 압축 프로세스(809)에서 이용되어야 할 장르, 압축 환경 및 압축 알고리즘이 검색된다, 단계(1304).

3. 컨텐츠 품질 제어 툴

컨텐츠 품질 제어 툴은 유저에게 전술된 것처럼 컨텐츠 품질 제어 프로세스(810)를 실행할 능력을 제공한다. 이것은 선택적인 컨텐츠 프로세싱 툴이며, 품질 제어 기술자에게 인코딩되고 워터마크된 컨텐츠 파일을 검토하게 하며, 품질 평가에 기초하여 이 컨텐츠 파일을 승인하거나 거절할 기회를 제공한다. 이 기술자는 품질이 적당하게 될 시까지 이 컨텐츠를 재인코딩하여 수동 전처리 조정을 하게하거나 또는 재처리용 노래를 플래그(flag)하며 이 문제를 설명하는 주석을 부착할 수 있다.

이러한 프로세스 단계는 컨텐츠 프로세싱 작업 흐름의 선택적인 단계 또는 필요한 단계로서 컨텐츠 제공자(들)(101)에 의해 구성될 수 있다. 부가적인 선택사항인 최종 품질 보증 프로세스(813) 단계는 이 컨텐츠에 대한 모든 SC(들)(예컨대, CD 상의 노래들에 대한 각각의 SC(들))를 패키징한 후에 제공되며, 이 때

에 컨텐츠 인코딩의 품질은 테스트될 수 있지만, 암호화 및 패키징에 앞서 문제를 이해함으로써 보다 효율적으로 컨텐츠를 프로세싱하게 한다. 따라서, 컨텐츠 품질은 이러한 단계에서 모든 프로세싱을 최종적으로 완성할 시 까지 기다리지 않는 것으로서 표명되는 것이 매우 바람직하다.

4. 암호화 툴

암호화 툴은 전술된 것처럼 암호화 프로세스(811)를 실행할 능력을 유저에게 제공한다. 컨텐츠 암호화는 컨텐츠 프로세싱 툴(155)의 마지막 단계다. 인코딩 툴이 생성하는 컨테츠 번전을 각각이 암호화된다. 암호화 툴은 SC 팩커(Packer)의 함수다. SC 팩커는 노래를 암호화하도록 호출되며, 생성되어 이용된 암호화 키를 반환한다. 이 키는 후에 메타데이터 SC(들)(620) 생성 시 이용하기 위해 SC(들) 팩커 내로 전달된다.

E. 컨텐츠 SC(들) 생성 툴

일단 모든 메타데이터가 컨텐츠 SC(들) 생성 툴로 수집되면, 메타데이터를 그들의 목적한 바대로 이용하기 위한 범주를로 그룹화한다. 이들 메타데이터 그룹들이 파일 내에 기록되어, 메타데이터 SC(들)(620)에 대한 메타데이터 부분들로서 SC(들) 팩커 툴로 전달된다. 각각의 부분(파일)은 독특한 프로세싱 요구들을 갖는다. 관련 노래들이 처리되어 암호화되고 그리고 타겟 목적지(컨텐츠 호스팅 사이트(들)(111)의 URL)가 결정된 경우, 컨텐츠(113)에 대한 컨텐츠 SC(들)(630)이 기꺼이 생성된다. 완벽하게 프로세싱하고 전술된 모든 요구들을 충족시키는 컨텐츠(113)가 작업 흐름 관리자(154)의 팩커 큐에 팩킹하기 위해 큐된다.

컨텐츠 SC(들) 생성 툴은 메타데이터 동화 및 진입 툴(161)의 이전 단계들이 생성한 요구되는 모든 파일들을 검색하며, SC(들) 팩커 함수를 호출하여 메타데이터 SC(들)(620) 및 컨텐츠 SC(들)(630)을 생성한다. 이 프로세스는 각각의 노래에 대해 단일 메타데이터 SC(들)(620) 및 다수의 컨텐츠 SC(들)(630)을 생성한다. 예를 들면, 컨텐츠가 음악인 경우, 완전한 노래의 다양한 품질 레벨들에 대한 오디오 프로세싱 동안 생성된 오디오 파일들 각각은 개별적인 컨텐츠 SC(들)(630)로 패킹된다. 샘플 클립에 대해 생성된 오디오 파일은 메타데이터 SC(들)(620)에 포함될 메타데이터 파일로서 전달된다.

F. 최종 품질 보증 툴

최종 품질 보증 툴은 전술된 것처럼 최종 품질 보증 프로세스(813)를 실행하는 능력을 유저에게 제공한다. 일단 모든 SC(들)이 컨텐츠 파일을 위해 구축되면, 이 컨텐츠는 최종 품질 보증 검사에 대해 이용될 수 있다. 품질 보증은 컨텐츠(113) 준비 프로세스의 다양한 단계들에서 실행될 수 있다. 컨텐츠 제공자(들)(101)는 각각의 주요한 단계가 나중에 지나친 재작업(rework)을 방지하도록 완성되기 때문에 품질을 보증하도록 선택할 수 있거나 또는 모든 오디오 준비 프로세스들이 완벽하여 한번에 모든 것들에 대한 품질을 보증할 시 까지 기다리도록 선택할 수 있다. 후자가 선택되는 경우, 품질 보증은 SC(들)의 생성을 완성하는 데로 이 지점에서 수행된다. 이 툴은 노래에 대한 각각의 SC(들)이 게방되어, 검사되고, 오디오 플레이되게 한다.

어떤 문제가 발견되는 경우, 마이너 텍스트 변화조차도 SC(들)이 SC(들)의 내부 안전 특성으로 인해 재구성될 것을 요구한다. 불필요한 재프로세싱 시간을 피하기 위해서, 일시적인 품질 보증 단계가 활용되어 메타데이터의 정확도를 보장하고 그리고 이 특정 품질 보증 단계가 이 노래와 관련있는 SC(들) 간의 적절한 상호 참조를 유효하게 하도록 예약되는 것이 권고된다. 문제들이 발견되는 경우, 보증자(assurer)는 문제에 대한 설명을 등록하여 노래에 부착시키며, 재프로세싱에 대한 적당한 프로세싱 큐에 다시 큐되게 한다. 상태가 작업 흐름 관리자(154)에서 적절히 갱신되어 관련된 모든 노래 구성요소들의 상태를 지시한다. 어떤 문제들도 발견되지 않는 경우, 컨텐츠(113)는 발매를 위해 준비된 데로 마크되거나 플래그된다.

G. 컨텐츠 배포 툴

컨텐츠 배포 툴은 전술된 것처럼 컨텐츠 배포 프로세스(814)를 실행할 능력을 유저에게 제공한다. 컨텐츠(113)가 배포를 위해 승인되면, 컨텐츠(113)에 대한 SC(들)은 컨텐츠 배포 프로세스의 큐에 배치된다. 컨텐츠 배포 툴은 큐를 감시하며, 컨텐츠 제공자(들)(101)이 제공한 구성 설정을 토대로하여 SC(들) 파일의 직접적인 전송 또는 SC(들) 파일 그룹들의 배치 전송을 실행한다. 컨텐츠 제공자(들)(101)은 컨텐츠 배포 툴을 선택적으로 구성하여 그들이 배포를 위해 수동으로 플래그될 시까지 모든 SC(들)을 이 큐에 자동으로 보유한다. 이것은 컨텐츠 제공자(들)(101)이 그들의 예정된 배포 날짜보다 미리 컨텐츠를 준비하게 하고 그리고 그들이, 예컨대 새로운 노래, 영화 또는 게임을 배포하기를 바랄 시 까지 그들을 보유하게 한다. SC(들)은 컨텐츠 제공자(들)(101)이 SC(들) 전달을 계속 유지하는데는 어떤 요구물도 필요가 없도록 정해진 배포 날짜를 토대로 컨텐츠(113)에 대한 엑세스를 제어할 수 있으며, 이러한 수동 배포 선택 사항은 이러한 목적을 위해 이용되거나 또는 이들 큰 파일들을 전송하는데 요구되는 네트워크 대역폭을 관리하는데 이용될 수 있다.

배포를 위해 플래그될 시, 컨텐츠(113)용 컨텐츠 SC(들)(630)은 FTP를 통해 정해진 컨텐츠 호스팅 사이트(들)(111)로 전달된다. 메타데이터 SC(들)(620)은 FTP를 통해 컨텐츠 판촉 웹 사이트(156)로 전달된다. SC(들)은 그들이 프로세싱되어 컨텐츠 판촉 웹 사이트(156)로 통합될 시 까지 새로운 컨텐츠(113) 디렉토리로 스테이징된다.

도 17은 본 발명에 따른 도 8의 자동 메타데이터 획득 툴에 대한 부가적인 정보를 자동으로 검색할 대체 실시예의 순서도다. 이 프로세스는 전술된 도 8에 기술된 것과 유사하다. 그러나, 강독된 배포(806)의 품질 검사 및 컨텐츠 품질 제어(809)는 품질 제어(1704)라 불리는 하나의 품질 검사로 결합된다. 메타데이터 SC 생성(807) 및 컨텐츠 생성(812)에 앞서 품질 검사를 수행한다. SC 생성에 앞서 품질 검사를 수행함으로써, 컨텐츠(113) 및 관련 메타데이터 SC(들)(620)를 패킹하지 않는 단계를 제거한다. 또한, 이 실시예에서, 제품들이 기다리는 동작/정보(801)의 큐가 제거된다. 어떤 동작이 요청되었는지에 따라 일들이 특정 프로세스 큐상에 배치된다. 예를 들면, 이 일이 수동 메타데이터, 즉 등록될 부가적인 메타데이터를 요구하는 경우, 이 일은 수동 메타데이터 등록 큐 상에 배치된다. 또한, 자동 메타데이터 획득(803)은 메타데이터 동화 및 진입 툴(161)과 컨텐츠 프로세싱 툴(155)에 앞서 발생하도록 새로운 컨텐츠 요청과 결

합된다. 마지막으로, 처리 조건(804)이 자동 메타데이터 획득(803)에서 그리고 수동 메타데이터 진입(803) 동안 등록되는 것을 주목하는 것은 중요하다. 다수의 처리 조건들이 자동 메타데이터 획득(803) 단계 동안 자동으로 채워질 수 있다.

H. 컨텐츠 판촉 웹 사이트

컨텐츠 제공자(들)이 디지털 다운로드를 통해 판매하기 위해 이용하는 정보를 가장 효과적으로 배포하기 위해서, 그리고 고객에게 다운로드하는데 이용될 수 있는 이러한 컨텐츠(113)를 만들도록 전자 디지털 컨텐츠 상점(들)(103)에 필요한 파일들을 얻기 위해서, 각 컨텐츠 제공자(들)(101)은 이러한 정보를 포함하는 안전한 웹 사이트를 가져야 한다. 이것은 이러한 정보를 필요로하는 소매업자들 및 다른 사람들에게 이용될 수 있는 판촉 컨텐츠를 만들기 위해 몇몇 컨텐츠 제공자(들)(101)이 현재 이용하는 방법과 유사하다. 이러한 서비스 유형이 이미 존재하는 경우에, 전자 디지털 컨텐츠 상점(들)이 다운로드를 통해 판매하는데 이용할 수 있는 컨텐츠 목록을 볼 수 있는 웹 사이트에 부가적인 부분이 부가될 수 있다.

컨텐츠 제공자(들)(101)은 이러한 사이트의 설계 및 레이아웃을 완벽히 제어하거나 또는 안전한 디지털 컨텐츠 전자 배포 시스템(100)용 툴킷의 부분으로 제공되는 턴키(turnkey) 웹 서버 솔루션을 이용하도록 선택할 수 있다. 이러한 서비스에 대해 자신이 설계하기 위해서, 컨텐츠 제공자(들)(101)은 그들의 사이트를 액세스하는 전자 디지털 컨텐츠 상점(들)(103)에 대한 메타데이터 SC(들)(620)에 링크하는 것을 필요로한다. 이것은 안전한 디지털 컨텐츠 전자 배포 시스템(100)에 대한 툴킷을 이용하여 수행된다. 선택 프로세스 및 어떤 정보가 도시되는 냐는 컨텐츠 제공자(들)(101)의 결정 사항이다.

컨텐츠 배포 툴로부터 FTP를 통해 새로운 컨텐츠 디렉토리 내로 수신된 메타데이터 SC(들)(620)은 컨텐츠 판촉 웹 사이트(156)에 의해 프로세싱된다. 이들 컨테이너는 컨테이너로부터 정보를 디스플레이하거나 추출하기 위해서 SC(들) 사전 검토 툴로 개방될 수 있다. 이 정보는 HTML 웹 페이지를 갱신하고 및/또는 정보를 이 서비스가 유지하고 있는 검색 가능한 데이터베이스로 부가하는데 이용될 수 있다. SC(들) 사전 검토 툴은 메타데이터 SC(들)(620)를 개방하고 프로세싱하기 위해서 전자 디지털 컨텐츠 상점(들)이 이용하는 컨텐츠 획득 툴의 부분집합이다. 보다 상세한 것은 컨텐츠 획득 툴부를 참조. 메타데이터 SC(들)(620) 파일은 컨텐츠 판촉 웹 사이트(156)가 유지하고 있는 영구 디렉토리로 이동되어야 한다.

일단 메타데이터 SC(들)(620)가 컨텐츠 판촉 웹 사이트(156) 내로 통합되면, 이것의 유용성이 공표된다. 컨텐츠 제공자(들)(101)은 각각의 새로운 메타데이터 SC(들)(620)가 사이트에 부가되기 때문에 가입하는 모든 전자 디지털 컨텐츠 상점(들)에 통지문을 전송할 수 있거나 또는 그날(또는 주기) 부가된 모든 메타데이터 SC(들)(620)에 대해 매일(또는 소정의 정의된 주기) 단 한번 통지할 수 있다. 이러한 통지문은 부가된 메타데이터 SC(들)(620)을 참조하는 매개변수들을 포함하는 정의된 CGI 스트링을 전송함으로써 전자 디지털 컨텐츠 상점(들)(103) 웹 서버를 사용하는 표준 HTTP 교환을 통해 수행된다. 이 메시지는 나중에 기술되는 전자 디지털 컨텐츠 상점(들)(103)의 통지문 인터페이스 모듈에 의해 다루어진다.

I. 컨텐츠 호스팅

오락 산업은 현재 가능한 수 만개의 컨텐츠 타이틀에 더하여, 매년 CDS, 영화 및 게임 등과 같은 컨텐츠 타이틀을 생산한다. 안전한 디지털 컨텐츠 전자 배포 시스템(100)은 상점이 이용할 수 있는 모든 컨텐츠 타이틀을 제공하도록 설계된다.

일상적인 기준에 따라 소비자들이 언젠가는 다운로드할 안전한 디지털 컨텐츠 전자 배포 시스템(100)의 수는 수천 혹은 수 만개이다. 대량의 타이틀에 의해, 이것은 많은 량의 대역폭이 필요하다. 컴퓨터 디스크 공간과 대역폭은 다중의 컨텐츠 호스팅 사이트(111)로 분배되어, 측량할 수 있는 수단을 필요로 한다. 상기 시스템은 또한 전 세계에 걸쳐 소비자를 지원한다. 이것은 전 세계의 소비자들에게 신속한 배달을 하기 위한 대외적인 사이트를 필요로 한다.

안전한 디지털 컨텐츠 전자 배포 시스템(100)상의 컨텐츠 호스팅은 다른 호스트에 컨텐츠 제공자(101) 자신의 컨텐츠(113)가 호환되도록 하거나 일반 시설(common facility)이나 시설의 설정을 공유한다.

안전한 디지털 컨텐츠 전자 배포 시스템(100) 상의 컨텐츠 호스팅은 안전한 디지털 컨텐츠 전자 배포 시스템(100)과 컨텐츠 제공자(101)에 의해 제공되어 현재 많은 접속 회수를 포함하는 몇몇 제 2 컨텐츠 사이트들(비도시)에 의해 제공된 모든 컨텐츠(113)를 일괄적으로 포함하는 다중의 컨텐츠 호스팅 사이트(111)로 구성한다. 컨텐츠 호스팅 사이트(111)의 수는 그 시스템을 이용하는 엔드 유저(End-User)의 수에 의존하여 변한다. 제 2 컨텐츠 사이트는 제한된 수의 노래를 호스트하지만, 그 사이트는 그 시스템에 이용되는 대역폭의 많은 부분에 상당할 것이다. 제 2 컨텐츠 사이트는 제 1 컨텐츠 사이트 상의 부피를 최대 수용 면에서 증가시킴으로써 온라인 상으로 가져온다. 제 2 컨텐츠 사이트는 다운로드 시간을 감소시키는데 유용한 네트워크 액세스 포인트(NAPs)에 근접하여 배치될 수 있다. 또한, 그 사이트는 다운로드 시간을 감소시키기 위해, 세계 곳곳의 다른 영역에 위치될 수도 있다.

컨텐츠 제공자(101)가 그들 자신의 시스템에서 그들의 모든 컨텐츠(113)를 호스트할 것을 선택하면, 그들은 부가적인 제 2 컨텐츠 사이트의 유무에 관계없이 단일 컨텐츠 호스팅 사이트(111)로서 작동할 수 있다. 이것은 그들 자신의 측량 가능한 분배 시스템을 세우기 위해 그들을 인정한다. 다른 실시예에서, 전자 디지털 컨텐츠 상점(103)은 임의의 컨텐츠(113)용의 컨텐츠 호스팅 사이트(111)로서 또한 작동할 수 있다. 이 실시예는 전자 디지털 컨텐츠 상점(103)과 컨텐츠 제공자(101) 간의 특수 금융 협약을 필요로 한다.

1. 컨텐츠 호스팅 사이트

컨텐츠(113)는 본 명세서의 컨텐츠 제공자 부분에서 기술된 컨텐츠 분배 툴에 의해 FTP나 HTTP를 매개로 하거나 테이프, CD ROM, 플래시나 다른 컴퓨터 판독 장치 상의 컨텐츠 전달과 같은 오프라인 수단을 매개로 하여 컨텐츠 호스팅 사이트(111)에 부가한다. 컨텐츠 제공자(101)에 의해 생성된 메타 데이터 SC(620)는 이 컨텐츠(113)를 위한 컨텐츠 SC(630)가 위치하는 URL을 가리키는 영역을 포함한다. 이 URL은 컨텐츠 호스팅 사이트(111)에 상응한다. 전자 디지털 컨텐츠 상점(103)은, 제의 SC(641) 내의 컨텐츠 제공자(101)에 의해 인정된다면, 이 URL을 우선시 할 수 있다. 엔드 유저 장치(109)는 컨텐츠 SC(630)를

다운로드 하기를 원할 때, 이 컨텐츠 호스팅 사이트(111)와 통신한다.

엔드 유저 장치(109)는 컨텐츠 호스팅 사이트(111)에 라이센스 SC(660)를 전송하는 것에 의해 컨텐츠 SC(630)의 요구를 시작한다. 이것은 결제소(105)에 의해 되돌아 온 동일 라이센스 SC(660)이다. 그것이 합법적인 라이센스 SC(660)라면, 라이센스 SC(660)의 디지털 서명을 결정하도록 사실임을 증명한다. 그것이 합법적인 라이센스 SC(660)라면, 다른 다운로드를 시작하거나, 다운로드 요구를 또 다른 컨텐츠 호스팅 사이트(111)에 다시 지시할 것이다.

2. 안전한 디지털 컨텐츠 전자 배포 시스템(100)에 의해 제공된 컨텐츠 호스팅 사이트(111)

안전한 디지털 컨텐츠 전자 배포 시스템(100)을 위해 컨텐츠(113)를 다운로드하는데 이용되는 사이트의 결정은 컨텐츠 SC(630)에 의해 최초 요구가 수신된 제 1 컨텐츠 사이트에 의해 이루어진다. 이 사이트는 이 결정을 하기 위한 다음의 정보를 이용한다.

· 컨텐츠(113)를 호스트할 제 2 컨텐츠 사이트가 요구되는가?(안전한 디지털 컨텐츠 전자 배포 시스템(100)에 의해 제공된 컨텐츠(113)의 대부분은 제 1 컨텐츠 사이트에만 위치된다.);

· 엔드 유저 장치(109)는 지리적으로 어디에 위치하는가?(이 정보는 요구가 엔드 유저 장치(109)에서 시작될 때, 엔드 유저 장치(109)로부터 얻을 수 있고, 이것은 주문 SC(650) 내에서의 결제소(105)까지 통과된다.);

· 적합한 제 2 컨텐츠 사이트를 동작시키는가?(때때로 제 2 컨텐츠 사이트는 오프라인이다.)

· 제 2 컨텐츠 사이트의 로드는 무엇인가?(제 2 컨텐츠 사이트가 덜 바쁜 다른 사이트의 활동에 쇄도되는 몇몇 경우에 선택될 것이다.)

엔드 유저 장치(109)에 컨텐츠 SC(630)를 전송하기 전에, 검토와 확인은 엔드 유저의 요구로 실행된다. 데이터 베이스는 다운로드 컨텐츠(113)에 이용되어 온 모든 라이센스 SC IDs를 유지한다. 이 데이터 베이스는 엔드 유저 장치(109)만이 구매된 각 컨텐츠(113)의 요구를 받아들여 확인하는 것에 의해 체크될 수 있다. 이것은 컨텐츠 호스팅 사이트(111)의 속도를 낮추기 위해 악의있는 사용자가 반복적으로 컨텐츠 호스팅 사이트(111)를 액세스하는 것을 방지한다.

제 2 컨텐츠 사이트에 대한 컨텐츠(113)의 증감은 개별 컨텐츠(113)의 소비자 요구에 근거하여 주기적으로 실행된다.

컨텐츠 호스팅 라우터(Content Hosting Router)

컨텐츠 호스팅 라우터(비도시)는 컨텐츠 호스팅 사이트(111) 내에 마련하고, 컨텐츠(113)를 다운로드하기 원하는 엔드 유저로부터 모든 요구를 수신한다. 그것은 그들이 정말로 컨텐츠(113)를 구매했는지를 확인하기 위해 엔드 유저 요구 상의 확인 검사(validation check)를 실행한다. 데이터 베이스는 컨텐츠(113)가 그들과 그들의 현재 상태가 어떤지를 포함하는 제 2 컨텐츠 사이트의 형태로 유지된다. 이 현재 상태는 사이트 상의 많은 동작과 사이트를 유지하기 위해 다운할지를 포함한다.

제 2 컨텐츠 사이트(Secondary Content Sites)

제 2 컨텐츠 사이트(비도시)는 안전한 디지털 컨텐츠 전자 배포 시스템(100)의 유명한 컨텐츠(113)를 호스트한다. 이들 사이트는 세계에 걸쳐 지리적으로 분산되고, 다운로드 시간을 향상시키기 위해 네트워크 액세스 포인트(NAPs) 가까이 위치시킨다. 이들 사이트는 최대 용량(maximum capacity)에 가까운 제 1 컨텐츠 호스팅 사이트(111) 상의 요구로서 시스템에 부가된다.

IX. 전자 디지털 컨텐츠 상점

A. 개요 - 다중 전자 디지털 컨텐츠 상점(103)을 위한 지원

전자 디지털 컨텐츠 상점(103)은 본래 소매상이다. 그들은 소비자에게 분배될 컨텐츠(113)를 판매한다. 컨텐츠(113)의 분배를 위해, 이것은 디지털 컨텐츠 소매 웹사이트, 디지털 컨텐츠 소매 상점 혹은 소비자에게 전자 컨텐츠(113)를 마케팅하는데 수반되기를 원하는 어떤 사업이라도 포함된다. 이들 사업은 전자 컨텐츠(113)의 판매만을 마케팅하거나 그들이 현재 판매하려고 하는 물품은 무엇이든지 전자 상품의 판매에 부가하는 것만으로 선택할 수 있다. 전자 디지털 컨텐츠 상점(103)이 제공하는 서비스에 다운로드 가능한 전자 상품의 정보는 안전한 디지털 컨텐츠 전자 배포 시스템(100)의 부분으로서 전자 디지털 컨텐츠 상점(103)에 의해 진보된 일련의 툴을 거쳐 성취된다.

이들 툴은 안전한 디지털 컨텐츠 전자 배포 시스템(100)에 의해 이하와 같이 이용된다.

· 컨텐츠 제공자(101)에 의해 패키징된 메타 데이터 SC(620)를 획득한다.

· 그들의 서비스 제안을 세우기 위해 입력으로 이용되는 이들 SC로부터 컨텐츠(113)를 추출한다.

· 판매를 위해 제안된 다운로드 가능한 컨텐츠(113)를 설명하는 제의 SC(641)를 생성한다.

· 판매의 승인과 엔드 유저 장치(109)에 트랜젝션 SC(640)을 생성하여 전송하는 것에 의해 다운로드의 시작을 제어한다.

· 다운로드 가능한 컨텐츠(113) 판매의 트랜젝션 기록과 각 다운로드의 상태를 유지한다.

· 상태 툴지와 트랜젝션 인증자 요구를 제어한다.

· 계정 조정을 실행한다.

이 툴은 전자 디지털 컨텐츠 상점(103)이 그것의 서비스에 다운로드 가능한 전자 컨텐츠(113)의 판매를 추가하기를 원하는 방법으로 유연성을 가지도록 설계된다. 이 툴은, 판매된 다운로드 가능한 컨텐츠(113)에 의한 모든 금융 사업이, 비록 결제소(105)가 필요 없을지라도, 결제소에 의해 조정되는 것

을 요구하는 방법과 같이 이용될 수 있다. 이들 툴은 또한 그들 소비자들에게 완벽한 서비스를 하기 위해 전자 디지털 컨텐츠 상점(103)을 이용하고, 프로모션의 제공과 특수한 제의를 포함하는 자체의 금융 트랜잭션을 조정한다. 이 툴은 그것이 가지고 있는 서비스에 다운로드 가능한 컨텐츠(113)의 판매를 빠르게 포함시키기 위해 전자 디지털 컨텐츠 상점(103)을 이용 가능하게 한다. 게다가 전자 디지털 컨텐츠 상점(103)은 다운로드 가능한 컨텐츠(113)를 호스트할 필요는 없고, 그것의 배치(dispersement)를 유지할 필요는 없다. 이 기능은 컨텐츠 제공자(101)에 의해 선택된 컨텐츠 호스팅 사이트(111)에서 실행된다.

전자 디지털 컨텐츠 상점(103)을 위한 툴은 바람직한 실시예에 있어서는 자바(Java)에 의해 실행되지만, C/C++, 어셈블러 및 그에 상응하는 것과 같은 다른 프로그램 언어도 사용될 수 있다. 전자 디지털 컨텐츠 상점(103)용의 후술하는 툴은 하드웨어와 소프트웨어 플랫폼의 여러 가지로 구동할 수 있다. 완전한 시스템이나 그것의 구성 요소 중 하나로서 전자 디지털 컨텐츠 상점(103)은 웹과 같이 전자 분배에 한정되는 것이 아니라, 플로피 디스켓, CD ROMS 및 삭제 가능한 디스크 드라이브를 포함하는 컴퓨터 판독 매체에 어플리케이션 프로그램으로서 분배될 수도 있다.

다른 실시예에서, 전자 디지털 컨텐츠 상점(103)의 구성요소는 프로그래머 소프트웨어 툴킷의 한 부분이다. 이 툴킷은 일반적인 전자 디지털 컨텐츠 상점(103)의 구성요소에 미리 정해진 인터페이스를 이용하게 하고 툴은 이하에 설명한다. 이들 미리 정해진 인터페이스는 APIs나 어플리케이션 프로그래밍 인터페이스의 형태이다. 이 APIs를 이용하는 개발자는 하이 레벨의 어플리케이션 프로그램으로부터 구성 요소의 어떤 기능이라도 발휘할 수 있다. 이들 구성 요소를 APIs로 제공하는 것에 의해, 프로그래머는 이들 기능을 재생성하고 이들 구성 요소의 어떤 자원도 필요로 하지 않고 빨리 원하는 전자 디지털 컨텐츠 상점(103)을 개발할 수 있다.

전자 디지털 컨텐츠 상점(103)은 서비스 제안에 근거한 웹에 한정되는 것은 아니다. 제공된 툴은 전송 인프라에 관계없이 다운로드 가능한 전자 컨텐츠(113)를 판매하기를 원하는 모든 전자 디지털 컨텐츠 상점(103)이나 이 컨텐츠(113)를 엔드 유저에 배달하기 위해 이용되는 배달 모드에 이용된다. 위성과 케이블 인프라를 거쳐 제공된 방송 서비스는 또한 전자 컨텐츠(113) 판매를 획득하고, 패키지하고 트랙(track)하기 위해 이들 동일 툴을 이용한다. 판매용 전자 상거래의 프리젠테이션과 이들 제의가 엔드 유저에 배달되는 방법은 서비스 제의에 근거한 방송과 포인트-투-포인트 상호 웹 서비스형 제의 사이의 주요한 변형이다.

B. 포인트-투-포인트 전자 디지털 컨텐츠 배포 서비스

포인트-투-포인트는 본래 전자 디지털 컨텐츠 상점(103)과 엔드 유저 장치(109) 간의 1대1 상호 서비스를 의미한다. 이것은 전형적으로 전화나 케이블 모뎀 접속을 통해 제공된 서비스에 근거하며 인터넷 웹을 나타낸다. 인터넷과는 달리 네트워크는, 그것이 웹서버/클라이언트 브라우저 모델을 확인하는 한, 이 모델로 또한 공급된다. 도 9는 주요 툴, 구성 요소 및 전자 디지털 컨텐츠 상점(103)의 프로세스를 설명하는 블록도이다.

1. 통합 요건

안전한 디지털 컨텐츠 전자 배포 시스템(100)은 새로운 온라인 비즈니스를 생성할 뿐만 아니라, 현재 발명에 다운로드 가능한 전자 컨텐츠(113)의 판매를 통합하도록 비즈니스하기 위한 방법을 제공한다. 전자 디지털 컨텐츠 상점(103)에 제공된 그 툴은 이 통합을 위한 수고를 단순화할 수 있다. 컨텐드 획득 툴(171)과 SC 패키징 툴(153)은 컨텐츠 제공자(101)가 판매할 수 있는 어떤 것인지에 대하여 관여하는 컨텐츠 제공자(101)로부터 정보를 획득하고, 그를 자신의 목록에서 상품으로서의 이들 다운로드 가능한 목적물에 필요한 파일을 생성하도록 전자 디지털 컨텐츠 상점(103)을 위한 방법을 제공한다. 이 프로세스는 배치 구동되어 폭넓게 자동화될 수 있으며, 사이트에 새로운 컨텐츠(113)를 통합할 때에만 실행된다.

안전한 디지털 컨텐츠 전자 배포용 툴은 전자 디지털 컨텐츠 상점(103)(예컨대, Columbia House online, Music Boulevard, @Tower)에 근거한 웹의 전형적인 방법과 파라다임을 소비하는 그룹의 현재 컨텐츠(113)에 최소한의 변화를 주는 것과 동등한 것으로 다운로드 가능한 전자 컨텐츠(113)의 판매를 통합시키도록 설계되고 있다. 통합의 몇 가지 방법은 바람직한 실시예에 의해 가능하고, 전자 디지털 컨텐츠 상점(103)은 모든 물품의 검색, 미리 보기, 선택(쇼핑 카트(shopping cart)) 및 구입 등의 지원(support)을 제공한다. 각 전자 디지털 컨텐츠 상점(103)은 소비자들과 소비자 로열티(customer loyalty)를 맺고, 물품의 판매에 따라 그 자신의 인센티브를 제의를 계속한다. 안전한 디지털 컨텐츠 전자 배포 시스템(100)에 있어서, 그 목록의 물품은 전자 다운로드가 가능하고, 구입을 선택했을 때, 그 소비자가 전자 다운로드 옵션을 선택하는 것을 허가하도록 지시할 것을 간단히 할 필요가 있다. 다른 실시예에서, 소비자의 쇼핑 카트는 전자 컨텐츠(113)의 혼합과 물리적인 매체 선택을 포함한다. 소비자가 체크 아웃한 후, 전자 디지털 컨텐츠 상점(103)은 금융 처리를 완결하고, 구입된 물품을 처리하도록 그것의 적재(shipping) 및 조정(handling) 기능, 즉 전자 디지털 컨텐츠 상점(103)의 교환 조정 기능(commerce handling function)을 로그하거나 통지하고 나서, 모든 전자 다운로드를 조정하도록 트랜잭션 프로세서 모듈(175)을 호출한다. 그것은 요청된 정보를 간단히 통과하여 그 위치로부터의 모든 처리는 안전한 디지털 컨텐츠 전자 배포 시스템(100)용의 툴셋에 의해 조정된다. 다른 실시예에서, 트랜잭션 핸들링의 다른 방법은 다운로드 가능한 물품만을 판매하거나 물리적이고 다운로드 가능한 물품의 금융 처리를 분리하기 원하는 전자 디지털 컨텐츠 상점(103)의 금융 처리를 조정하기 위해 안전한 디지털 컨텐츠 전자 배포 시스템(100)용의 툴을 이용하는 것도 또한 가능하다.

물품의 다운로딩을 조정하기 위해, 전자 디지털 컨텐츠 상점(103)은 컨텐츠 제공자(101)용의 컨텐츠 프로모션 웹사이트(156)로부터 입수되는 각 다운로드 가능한 물품용의 상품 ID(비도시)가 주어진다. 이 상품 ID는 다운로드 가능한 물품과 소비자의 구입 선택을 연결시켜준다. 상품 ID는 사용자가 구매하려는 상품을 확인하기 위해 전자 디지털 컨텐츠 상점(103)이 트랜잭션 프로세서 모듈(175)을 통과한 것이다. 상품을 설명하기 위해 생성된 SC(제의 SC(641))는 전자 디지털 컨텐츠 상점(103)으로부터 분리되고, 이들 목적물을 간단히 유지하기 위해 제의 데이터 베이스(181) 내에 유지하며, 그들의 존재를 전자 디지털 컨텐츠 상점(103)에 반영하게 한다.

트랜잭션 프로세서 모듈(175)과 다른 부가적인 기능은 실행 가능한 웹서버 혹(예컨대. CGI와 NSAPI,

ISAPI를 호출 가능한 기능)이나 간단히 DLL이나 C 오브젝트 라이브러리에 APIs를 제공한다. 이들 기능은 엔드 유저 상호 작용과 결제소(105)와의 부가적인 상호 작용을 처리하는 구동 시간을 조정한다. 이들 기능은 웹서버의 교환 서비스를 생성하도록 상호 작용하고 컨텐츠(113) 다운로드 처리를 시작하는데 필요한 파일을 엔드 유저 장치(109)로 다운로드한다. 그들은 또한 권한 부여(authorizations)를 제공하기 위해 부가적인 상호 작용을 조정하고 동작 완료의 통지를 받아들인다.

계정 조정 툴(179)은 또한 그 자신에 근거한 계정과 결제소(105)의 트랜젝션 로그를 조정하기 위해 결제소(105)를 접속하는데 전자 디지털 컨텐츠 상점(103)을 보조하도록 제공된다.

2. 컨텐츠 획득 툴(171)

컨텐츠 획득 툴(171)은 메타 데이터 SC(620)를 미리 보기하고 다운로드하도록 컨텐츠 프로모션 웹사이트(156)를 인터페이스해야 한다. 컨텐츠 프로모션 웹사이트가 표준 웹사이트이므로, 웹브라우저는 이 사이트를 네비게이트하도록 전자 디지털 컨텐츠 상점(103)에 의해 이용된다. 네비게이션 형태는 컨텐츠 제공자(101)의 사이트 설계에 근거하여 변화한다. 몇몇 사이트는 촉진적인 정보의 많은 스크린으로 확장된 검색 능력을 제공할 수도 있다. 다른 것은 타이틀 목록, 실행자(performer) 혹은 선택될 새로운 릴리스(release)의 인터페이스를 가질 수도 있다. 모든 사이트는 노래나 앨범의 촉진적이고 기술적인 모든 정보를 포함하는 메타 데이터 SC(620)의 선택을 포함한다.

전자 디지털 컨텐츠 상점(103)은 업데이트 목록을 기재하고 FTP를 거쳐 자동적으로 업데이트를 수신할 수도 있다.

메타 데이터 보기

컨텐츠 획득 툴(171)은 메타 데이터 SC(620) 링크가 컨텐츠 프로모션 웹사이트(156)에서 선택할 때마다 런치(launch)하는 웹브라우저 보조 어플리케이션이다. SC의 선택은 그것이 전자 디지털 컨텐츠 상점(103)에 다운로드되도록 하고, 보조 어플리케이션을 런치한다. 컨텐츠 획득 툴(171)은 메타 데이터 SC(620)를 오픈하고, 거기에 포함된 비암호화 정보를 표시한다. 표시된 정보는 음악 샘플, 그 음악과 관련된 그래픽 이미지와 그 음악에 관한 정보, 그 음악을 또한 들을 수 있는 미리 보기 클립과 같은 정보가 포함된 확장된 메타 데이터를 포함한다. 컨텐츠(113)가 음악인 것을 예로 들면, 컨텐츠 제공자(101)에 의해 제공만 된다면, 노래나 앨범에 대한 촉진적인 정보, 앨범 타이틀 및 가수를 또한 보여준다. 이 정보는 브라우저 창에서 링크된 일련의 HTML 페이지에 의해 나타낸다. 노래와 가사(lyric)와 같이 판매 가능한 컨텐츠(113)와 컨텐츠 제공자(101)가 보호하기 바라는 다른 메타 데이터는 무엇이든지 소매 컨텐츠 웹사이트(180)에 액세스할 수 없다.

다른 실시예에서, 컨텐츠 제공자(101)는 비용에 관한 부가적인 촉진 컨텐츠를 제공한다. 이 실시예에서 촉진 컨텐츠는 메타 데이터 SC(620)로 암호화된다. 이 데이터를 오픈하기 위한 금융 처리는 선택된 비용이 변화되는 전자 디지털 컨텐츠 상점(103)의 계정을 결제소(105)를 거쳐 조정할 수 있다.

추출 메타 데이터

미리 보기 기능에 더하여, 이 툴은 두 개의 부가적인 형태, 즉, 메타 데이터 추출 및 제의 SC(641)의 준비를 제공한다. 메타 데이터 추출 옵션의 선택은 메타 데이터가 저장될 경로와 파일명을 입력하도록 전자 디지털 컨텐츠 상점(103)에 촉구한다. 그래픽과 오디오 미리 보기 클립과 같은 2진 메타 데이터는 별도의 파일로서 저장된다. 문자 메타 데이터는 소매 컨텐츠 웹사이트(180)가 그 데이터 베이스를 입수할 수 있는 제한된 ASCII 텍스트 파일로 저장된다. 제한된 ASCII 텍스트 파일의 레이아웃을 기술하는 테이블은 별도의 TOC 파일에서 또한 생성된다. 부가적인 옵션은 포맷이 제공된 다른 NLS(National Language Support)에 추출을 허가할 수 있다.

추출된 데이터에 제공된 가장 중요한 정보 중 하나는 상품 ID이다. 이 상품 ID는 전자 디지털 컨텐츠 상점(103)용 교환 조정 기능이 사용자가 구매하려는 컨텐츠(113)를 트랜젝션 프로세서 모듈(175)(트랜젝션 프로세싱부에 더 많은 정보를 제공하기 위함)에 확인하기 위해 필요한 것이다. 트랜젝션 프로세서 모듈(175)은 엔드 유저 장치(109)에 뒤이은 다운로드를 위해 제의 데이터 베이스(181)로부터 적합한 제의 SC(641)를 적절히 정정하기 위해 이 상품 ID를 사용한다. 전자 디지털 컨텐츠 상점(103)은 그 사이트 상에 다운로드 가능한 컨텐츠(113)의 제의를 어떻게 나타낼지 전체적으로 제어한다. 그것은 단지 안전한 디지털 컨텐츠 전자 배포 시스템(100)용의 툴로 적절하게 인터페이스하기 위해, 이 상품 ID로 제안된 컨텐츠(113)의 상호 참조(cross reference)를 유지할 필요가 있다.

여기서 ID 정보를 제공하면, 그 목록에 이 상품이나 컨텐츠(113)를 통합하도록 전자 디지털 컨텐츠 상점(103)을 인정하고, 제의 SC(641) 생성 처리와 나란히 페이지(데이터 베이스)를 판매하므로 양 처리는 상품을 참조하는데 동일 상품 ID를 이용한다. 이것에 대한 내용은 이하에서 기술한다.

제의 SC(s) 생성 패키징(153)

전자 디지털 컨텐츠 상점(툴)(103)은 판매하는 다운로드 가능한 컨텐츠(113)를 기술하는 제의 SC(s)(641)을 생성하는데 필요하다. 제의 SC(s)(641)로 전달되는 대부분의 정보는 메타데이터 SC(s)(620)로부터 전달된다. 컨텐츠 획득 툴(171)은 이하와 같은 것에 의해 제의 SC(s)(641)를 생성한다.

· 메타데이터 SC(s)(620)내의 제의 SC(s) 템플레이트(template)에 의해 정의된 바와 같이 제의 SC(s)(641) 내에 포함되는데 필요하지 않는 부분을 메타데이터 SC(s)(620)에서 제거

· 전자 디지털 컨텐츠 상점(툴)(103)용 이 툴내의 구성요소 옵션에 의해 특정지어 지는 디폴트들에 의해 정의된 바와 같이 추가의 요구 부분을 부가

· 메타데이터 SC(s)(620) 내의 제의 SC(s) 템플레이트에 의해 정의된 바와 같이 추가 요구 입력들 또는 선택들에 대한 판촉

· 이 정보를 패키징하기 위해 SC(s) 패킹(153)을 SC(s) 포맷으로 호출

엔드-유저 장치(들)(109)상의 재생기 애플리케이션(195)(이하에서 더 설명함)에 의해 디스플레이될 메타데이터를 메타데이터 SC(s)(620)내에 유지한다. 그것의 웹 서비스 데이터베이스로의 입력으로서, 전자 디지털 컨텐츠 상점(들)(103)에 의해서만 이용되는 다른 판촉 메타데이터만이 메타데이터 SC(s)(620)로부터 제거된다. 또한, 워터마킹 지시(Instructions), 암호화 대칭 키들(623) 및 객체의 허용된 사용임을 정의하는 사용 조건(517)과 같은, 컨텐츠 제공자(들)(101)에 의해 제공되는 권리 관리 정보도 유지된다.

이때, 제거된 메타데이터 SC(s)(620)은 제의 SC(s)(641) 내에 포함된다. 전자 디지털 컨텐츠 상점(들)(103)은 소위 상점 사용 조건들(519)라 불리는 그 자신의 사용 조건 또는 오퍼 SC(s)(641)에 대한 구매 옵션을 또한 첨부한다. 이것은 디폴트의 세트를 통해 상호적으로 또는 자동적으로 성취될 수 있다. 처리될 구성 요소가 상호적이라면, 전자 디지털 컨텐츠 상점(들)(103)은 컨텐츠 제공자(들)(101)에 의해 정의된 바와 같이 허용된 객체 사용 조건(517)의 세트에 의해 즉시 실행할 수 있다. 고객은, 이때 그 고객들에게 제의되는 옵션(들)을 선택한다. 이것들은 즉시 새로운 사용 조건들 또는 상점 사용 조건들(519)로 된다. 자동적으로 처리하기 위해서는, 전자 디지털 컨텐츠 상점(들)(103)이 모든 컨텐츠(113)에 대해 제의될 디폴트 구매 옵션들의 세트로 구성된다. 이들 디폴트 옵션들은 컨텐츠 제공자(들)(101)에 의해 정의된 허용 사용 조건들(517)에 대응하여 자동적으로 체크되고, 불일치가 없으면, 제의 SC(s)(641)내에서 세트화된다.

일단 제의 SC(s)(641)가 생성되면, 제의 데이터베이스(181) 내에 저장되고, 메타데이터 SC(s)(620) 내에 사전 부여된 제품(product) ID로 인덱싱된다. 이 제품 ID는, 엔드-유저(들)에게 패키징하기 위한 제의 SC(s)(641)를 유지하기 위해 제의 데이터베이스(181)로 인터페이싱하며 엔드-유저(들)에게 전송할 때, 다운로드 가능한 컨텐츠(113)를 식별하기 위하며, 이후에 전자 디지털 컨텐츠 상점(들)(103)에 의해 사용된다. 더 상세히는 트랜잭션 처리기 모듈(175)을 참조하라.

또다른 실시예에 있어서, 전자 디지털 컨텐츠 상점(들)(103)은 그의 사이트에서 컨텐츠 SC(s)를 호스팅한다. 이 실시예에서는 전자 디지털 컨텐츠 상점(들)(113)의 URL로 컨텐츠 호스팅 사이트(들)(111)의 URL의 대치와 같은 제의 SC(s)(641)를 변화시키는데 필요하다.

3. 트랜잭션 처리 모듈(175)

전자 디지털 컨텐츠 상점(175)은 결산서를 발송하도록 결제소(들)(105)에게 지시한다. 이와 달리, 전자 디지털 컨텐츠 상점(들)(103)이 결제소(들)(105)에서 직접 금융 결제를 요청할 수도 있다. 엔드-유저(들) 구매를 처리하기 위한 이 두개의 기본 모드는 다운로드 가능한 컨텐츠(113)를 필요로 한다. 전자 디지털 컨텐츠 상점(들)(103)이 구매에 대한 금융 결제 조정을 실행하기를 원하지 않아 상품의 판매를 결정하는 특정 판촉 행위나 인센티브(incentive)가 없고 구매 요구를 일괄 처리하는 쇼핑 카트 메타포어(metaphor)를 사용하지 않는다면, 제의 SC(s)(641) 파일에 직접 페이지들을 다운로드 가능한 그 컨텐츠(113)상으로의 링크를 제공하는 것을 선택할 수도 있다. 이를 제의 SC(s)(641)는 메타데이터 내에 포함된 소매 가격 정보를 만들어 놓도록 해야 한다. 또한, 판매 기간 및 조건을 갖는 구매 옵션들을 표현하는 페이지를 제공하는 특정 HTML이 제의 SC(s)(641)내에 포함되어야 한다. 이 페이지는 제의 SC(s)(641)이 만들어 질 때 생성된 템플레이트로부터 생성된다. 엔드-유저(들)가 제의 SC(s)(641)에 직접 링크하기 위해 클릭할 때, 제의 SC(s)(641)은 컨테이너를 개방하여 제의 SC(s)(641) 내에 포함된 제의 페이지들을 표시하는 헬퍼 애플리케이션을 개시하는 엔드-유저 장치(들)의 브라우저로 다운로드된다. 이 페이지에는 신용 카드 정보 및 구매 옵션 선택을 포함하는 고객 정보를 선택하기 위한 형태가 포함되어 있다. 이 형태는 금융 결제용 결제소(들)(105)에게 직접 제출되어 처리된다. 선택적으로, 이 형태는 엔드-유저(들)의 신용 정보 또는 자본 표준 로컬 트랜잭션 핸들러를 사용하는데 필요한 분야를 포함하고 있다.

전자 디지털 컨텐츠 상점(들)(103)이 계산서를 조정하는 실시예를 지금 설명한다. 구매 요구를 조정하는 더 많은 특정 모드는 전자 디지털 컨텐츠 상점(들)(103)이 금융 결제 처리를 허용하는 것이어서 이후, 다운로드 인증을 엔드-유저(들)에게 허여한다. 이 방법은, 전자 디지털 컨텐츠 상점(들)(103)이 그 사이트에서 판매를 제의하는 다른 상품을 갖는 다운로드 가능한 컨텐츠(113)의 판매를 통합하도록 허용하고, 각각 다운로드 요구를 제각기 변화하는 대신에 단지 하나의 통합된 변화로의 구매 요구를 처리하는 유용을 고객에게(쇼핑 카트 메타포어를 통해) 허용하며, 전자 디지털 컨텐츠 상점(들)(103)을 그 고객 구매 패턴을 직접 추적하도록 허용하며 특정 판촉 및 클럽 옵션들을 제공한다. 이러한 환경 하에서, 다운로드 가능한 컨텐츠(113)의 제의는 엔드-유저(들)에 의해 선택될 때, 쇼핑 카트에 추가되어 처리되는 고객의 쇼핑 페이지에 포함되고, 전자 디지털 컨텐츠 상점(들)(103)의 현재 쇼핑 모델 내에 수행되는 가격이 정해진다. 일단 금융 결제가 완료되면, 전자 디지털 컨텐츠 상점(들)(100)의 거래 조정 처리가 트랜잭션을 완료하기 위해 트랜잭션 처리기 모듈(175)을 호출한다.

트랜잭션 처리 모듈(175)

트랜잭션 처리 모듈(175)의 역할은 엔드-유저 장치(들)에 의해 필요한 정보를 함께 개시하도록 놓는 것이며, 구매한 컨텐츠(113)의 다운로드를 처리한다. 이 정보는 구매 제출에 대응하기 때문에 웹 서버에 의해 엔드 유저 장치(들)(109)로 되돌리는 트랜잭션 SC(s)(640)로 패키징된다. 트랜잭션 처리기 모듈(175)은 전자 디지털 컨텐츠 상점(들)(103)의 거래 조정 처리로부터의 세 가지 정보, 즉 구매한 컨텐츠(113)용 제품 ID들, 트랜잭션 데이터(642) 및 구매 결제를 확인하는 HTML 페이지 또는 CGI URL이 필요하다.

제품 ID는 메타데이터 SC(s)(620) 내에서 전자 디지털 컨텐츠 상점(들)(103)에 제공되는 판매 컨텐츠(113)와 연관되는 값이다. 이 제품 ID는 연관되는 제의 SC(s)(641)을 제의 데이터베이스(181)로부터 검색하는데 사용된다.

트랜잭션 데이터(642)는 이후에 전자 디지털 컨텐츠 상점(들)(103)에 의해 수행되는 금융 결제 트랜잭션을 처리하는 결제소(들)(105)와의 연관에 사용되는 전자 디지털 컨텐츠 상점(들)(103)의 트랜잭션 처리 기능에 의해 제공되는 정보의 구조이며, 엔드-유저 장치(들)(109)에 다운로드되는 컨텐츠(113)의 워터마크내에 포함될 사용자 식별 정보를 제공하는 것이다. 결제소(들)(105)가 유효 명령 SC(s)(650)를 수신할 때, 판매된 컨텐츠(113)를 지시하는 트랜잭션을 로그하며, 전자 디지털 컨텐츠 상점(들)(103)이 그것과

엔드-유저 이름 및 트랜잭션 ID(535)를 포함하는 연관 트랜잭션 데이터(642)를 판매한다. 이 트랜잭션 ID(535)는 금융 결제 트랜잭션의 증명서를 제공한다. 이 정보는 이후에 결제소(들)(105)에 의해 컨텐츠 제공자(들)(101)(또는 그 에이전트)로부터 수신된 계산서 상태와 그것의 계수를 증재하는데 사용하는 전자 디지털 컨텐츠 상점(들)(103)에게 회수된다. 결제소 트랜잭션 로그(178)는 컨텐츠 제공자(들)(101)에 의해 그 컨텐츠(113)가 판매되어 소유자의 로열티에 대한 각 전자 디지털 컨텐츠 상점(들)(103)에게 계산서를 생성하는데, 그것을 이용할 수 있도록 결정하는데 사용될 수 있다. 계산서를 제외한 다른 전자 결제 수단은 컨텐츠 제공자(들)(101)와 전자 디지털 컨텐츠 상점(들)(103) 사이의 결제 계수에 선택적으로 이용할 수 있다.

이 정보는 트랜잭션 SC(s)(640) 내에 제공되며, 트랜잭션 SC(s)(640)의 안전성 및 무결성이 결제소(들)(105)에 구매 트랜잭션의 유효함과 충분한 신뢰성을 제공하며, 더 이상의 유효성이 결제소(들)(105)에 의한 이러한 판매의 로깅에 우선하여 요구되지 않는다. 그러나, 전자 디지털 컨텐츠 상점(들)(103)은 그 계정이 변화되기 전에 입증서를 요구하는 옵션을 포함한다(결제소(들)(105)에서 로그된 이 전자 디지털 컨텐츠 상점(들)(103)이 이 컨텐츠(113)의 판매에 따른 수입을 가진 컨텐츠 제공자(들)(101)에게 지시하는 결제소(들)(105)로의 로그된 트랜잭션). 입증서/통지서에 대한 이러한 요구는 트랜잭션 데이터(642) 내의 플래그(flag)에 의해 지시된다. 이러한 시나리오에 있어서, 결제소(들)(105)는 전자 디지털 컨텐츠 상점(들)(103)과 접속하며, 그 계정에 대한 변화 및 암호화 키(623)의 양도 전에 전자 디지털 컨텐츠 상점(들)(103)으로부터 인증서를 수신한다. 트랜잭션 ID(535)는 엔드-유저(들)와 실행되는 최선 트랜잭션에 대해 이 요건을 전자 디지털 컨텐츠 상점(들)(103)과 연관시킬 수 있도록 이 입증서 요건의 일부분으로 결제소(들)(105)에서 전자 디지털 컨텐츠 상점(들)(103)으로 진행된다. 이 트랜잭션 ID(535)는 어떤 고유의 값일 수 있으며, 전자 디지털 컨텐츠 상점(들)(103)은 트랜잭션 ID를 사용하기를 원하며 오로지 그것에 대한 수익용이다.

트랜잭션 데이터(642)는 또한 고객 이름을 포함하고 있다. 이 이름은 구매서를 작성할 때 사용자에 의해 가재되는 구매 작성서의 사용자 이름 영역으로부터 파악할 수 있거나, 전자 디지털 컨텐츠 상점(들)(103)에 어떤 사용자가 등록하는 동안에 미리 로그된 정보로부터 파악할 수 있거나, 이 트랜잭션에 사용된 카드와 연관된 신용 카드 정보로부터 얻어지는 공인된 이름으로부터 파악할 수도 있다. 이 이름은 이후에 라이센스 워터마크(527)내에 포함된다.

또한, 트랜잭션 데이터(642)는 엔드-유저(들)에 의해 구매되는 상점 사용 조건(519)을 포함하고 있다. 이 정보는 라이센스 워터마크(527) 내에 포함되며, 카피 및 재생 제어에서 엔드-유저 장치(들)에 의해 이용된다.

트랜잭션 처리기 모듈(175)에 의해 요구되는 최종 파라메터는 구매 결제를 확인하는 HTML 페이지 또는 CGI URL이다. 이에 대한 목적은 금융 결제 및 응답 내에 포함하길 원하는 어떠한 정보의 확인에 대한 전자 디지털 컨텐츠 상점(들)(103)을 엔드-유저(들)에게 응답하도록 한 것이다. 이 HTML 페이지 또는 CGI URL은 트랜잭션 SC(s)(640) 내에 포함되고, 트랜잭션 SC(s)(640)가 수신되어 처리될 때 엔드-유저 장치(들)(109)의 브라우저 윈도우에 디스플레이된다.

이 트랜잭션 SC(s)는 구매서 제출을 처리한 후에 전자 디지털 컨텐츠 상점(들)(103)으로부터 엔드-유저(들)에 응답하는 HTTP이다. 직접 HTTP 응답으로써 SC(s)의 전송은 SC(s) 처리기 헬퍼 애플리케이션의 엔드-유저 장치(들)(109) 상에 자동 로딩을 강요하며 동작을 개시하고, 또한 엔드-유저(들)의 의존없이 트랜잭션의 자동 종료를 허용한다. 이 처리는 이후의 엔드-유저 장치(들)(109) 및 재생기 애플리케이션(195) 섹션에서 더 상세히 설명한다.

트랜잭션 처리기 모듈(175)이 요구하는 파라메터들을 호출할 때, 트랜잭션 데이터(642)를 포함하는 트랜잭션 SC(s)(640)을 생성하고, 레퍼런스 URL 또는 트랜잭션 인증 HTML, 다른 요구된 SC(s)의 안전한 특징, 구매와 연관된 제의 SC(s)(641)을 검색하며 삽입한다. 이것은 또한 통지 인터페이스 모듈(176) 및 계정 조정 툴(179)에 의해 이후에 이용하는 이 트랜잭션에 대해 정보를 로그한다.

4. 통지 인터페이스 모듈(176)

통지 인터페이스 모듈(176)은 웹 서버측의 실행 가능한 루틴(CGI 또는 NSAPI, ISAPI 등)에 의해 호출 가능한 기능)이다. 이것은 결제소(들)(105), 엔드-유저 장치(들)(109), 컨텐츠 호스팅 사이트(들)(111) 및 컨텐츠 제공자(들)(101)로부터 옵션 요구 및 통지를 조정한다. 전자 디지털 컨텐츠 상점(들)(103)이 임의로 통지 요구의 이벤트는

· 엔드-유저 장치(들)(109)가 암호화 키(623) 및 결제소(들)(105)를 요구하는 결제소(들)(105)로부터의 통지는 특정 컨텐츠(113)용 암호화 키(623)를 해제하는 것이다. 이러한 통지는 엔드-유저 장치(들)(109)로 전달되는 암호화 키(623) 이전에 전자 디지털 컨텐츠 상점(들)(103)으로부터 임의로 입증서를 요구하는 구성으로 될 수 있다.

· 컨텐츠 SC(s)(630)이 엔드-유저 장치(들)(109)에게 전송되는 컨텐츠 호스팅 사이트(들)(111)로부터의 통지

· 컨텐츠 SC(s)(630) 및 라이센스 SC(s)(660)이 수신되어 컨텐츠(113)를 성공적으로 처리하는데 이용되거나 손상됨을 발견되는 엔드-유저 장치(들)(109)로부터의 통지

· 새로운 컨텐츠(113)가 컨텐츠 판촉 웹 사이트(156) 내에 위치하는 컨텐츠 제공자(들)(101)로부터의 통지

이다.

이러한 통지가 안전한 디지털 컨텐츠 전자 배포 시스템 흐름(100)에서의 요구 단계이지만, 전자 디지털 컨텐츠 상점(들)(103)를 판매 완료의 만족을 기록에 근접시키도록 그 기회를 허용하는 옵션으로써 제공된다. 이것은 트랜잭션의 금융 결제 때문에 발생되는 어떠한 기능 또는 판매의 완료를 시도하는 동안 발생되는 어떠한 에러로 알려진, 전자 디지털 컨텐츠 상점(들)(103)을 임대함으로써 요청되는 고객 서비스를

조정하는데 필요한 정보를 또한 제공한다. 이와 달리, 대부분의 이들 상태는 필요한 만큼 고객 서비스 인터페이스(184)를 통해 결제소(들)(105)로부터 획득될 수 있다.

컨텐츠 판촉 웹 사이트(156)에서 유용한 새로운 컨텐츠(113)의 통지 빈도는 컨텐츠 제공자(들)(101)에 의해 결정된다. 각각 새로운 메타데이터 SC(s)(620)으로써 제공될 수 있는 통지는 그 날 추가된 새로운 모든 메타데이터 SC(s)(620)을 추가하는 동안이거나 단지 하루 동안만이다.

엔트리들 내의 이러한 모든 통지 결과는 트랜잭션 로그(178)에서 생성된다. 전자 디지털 컨텐츠 상점(들)(103)이 이러한 통지에서 그 소유 처리를 수행하기를 원한다면, 소유자는 CGI 호를 방해하고, 그 고유의 기능을 수행하여 통지 인터페이스 모듈(176)에서의 요청을 임의로 패스시킨다.

5. 계정 조정 툴(179)

이 계정 조정 툴(179)은 트랜잭션 로그(178)와 결제소(들)(105)의 로그와 비교하기 위해 결제소(들)(105)와 접속한다. 이것은 안전한 디지털 컨텐츠 전자 배포 시스템(100)에 대해 계정하는데, 안정감을 파악하는 전자 디지털 컨텐츠 상점(들)(103)를 도와주는데 유용한 임의의 처리이다.

또다른 실시예에 있어서, 이 툴은 컨텐츠 제공자(들)(101) 및 결제소(들)(105)에 자동 주기 지불을 위해 전송되는 전자 펀드를 제공하는데 업데이트될 수 있다. 이것은 트랜잭션 로그(178)에 대응하여 계산서를 조정한 후에 결제소(들)(105)로부터 전자 계산서의 수신으로 인해 지불을 자동적으로 처리하도록 설계될 수 있다.

C. 브로드케스트 전자 디지털 컨텐츠 배포 서비스

브로드케스트는 본래 주문형 영상 및 음성을 주문하기 위해 엔드-유저 장치(들)(109)와 전자 디지털 컨텐츠 상점(들)(103) 간의 사전 상호작용이 없는 많은 전송 방법의 하나로 언급된다. 이것은 통상적으로 컨텐츠(113)가 사전 프로그램 가능하여 모든 엔드-유저 장치(들)(109)가 동일 스트림을 수신하는 디지털 위성 또는 케이블 인프라를 통해 제공된다.

하이브리드 모델은 사이트 디자인에 대해 상당한 공유성을 갖도록 인터넷 접속은 물론 더넓은 밴드폭을 경유하는 웹 배포 인터페이스 또는 브로드케스트 서비스를 경유하는 케이블 배포 인터페이스를 양쪽다 제의하는 방법으로 구성되는 디지털 컨텐츠 서비스를 전자 디지털 컨텐츠 상점(들)(103)이 제공하도록 또한 정의될 수 있다. IRD 백채널 시리얼 인터페이스가 웹에 접속되어 IRD가 웹 네비게이션을 지지하면, 구매를 위해 컨텐츠(113)를 사전 검토 및 선택하는 엔드-유저(들)는 백채널 인터넷 인터페이스를 경유하는 통상의 방법으로 디지털 컨텐츠 서비스를 조정한다. 유저는 고품질의 다운로드 가능한 컨텐츠(113)를 선택할 수 있어 이러한 선택에 따라 구매하며, 인터넷 접속을 경유하여 요구하는 모든 라이센스 SC(s)(660)를 수신하여, 더 넓은 밴드폭을 갖는 브로드케스트용 인터페이스를 거쳐 컨텐츠(113)(컨텐츠 SC(s)(630))의 전달을 요구한다. 웹 서비스는 컨텐츠(113)가 브로드케스트 스케쥴에 근거하는 방식으로 다운로드할 수 있고, 또는 구매된 컨텐츠(113)를 근거하여 전체적으로 브로드케스트 스트림을 생성할 수 있다. 이 방법은 웹 근거 디지털 컨텐츠 서비스를, 이와 같은 방법으로 매일 유용한 제한 수의 특정 컨텐츠(113)(예컨대, 노래 또는 CD들) 및 웹 인터페이스를 경유하여 저품질로 다운로드하는데 유용한 전체 카탈로그를 생성하는 적당한 설비를 설치한, 고품질의 컨텐츠(113)를 유저들에게 전달하기 위한 브로드케스트 설비와 결합하도록 허용한다.

다른 방송용 모델들은 엔드-유저 장치(들)(109)를 위한 웹 서비스가 제공되지 않도록 설계될 수도 있다. 이 모델에 있어서, 판촉 컨텐츠는 스트림을, 특정 처리가 스트림을 디코딩하도록 수행되어, 구매 선택이 생성될 수 있는 판촉 컨텐츠로 엔드-유저(들)를 나타내는 엔드-유저 장치(들)(109)(즉, IRD)에게 전달하는 브로드케스트용 특정 포맷의 디지털 스트림으로 패키징된다.

실제 구매 선택은 백채널 커뮤니케이션을 경유하여 엔드-유저 장치(들)(109)로부터 결제소(들)로 여전히 초기화될 수 있어, 모든 데이터 변환을 수행하는데 SC(s)를 이용할 수 있다. 전자 디지털 컨텐츠 상점(들)(103)에 제공되는 이 툴세트는 포인트-투-포인트 인터넷 서비스 제의뿐만 아니라 브로드케스트용 위성 또는 케이블 제의 양쪽에 대해 대부분의 툴을 제공하는 방법으로 구조 설계 및 개발되어 왔다. 컨텐츠(113)를 획득하여 관리하는 것뿐만 아니라 SC(s)를 준비하는 디지털 컨텐츠 웹 사이트 전자 디지털 컨텐츠 상점(들)(103)에 의해 이용되는 툴들은 브로드케스트 인프라로 배포하기 위해 컨텐츠(113)를 관리하여 준비하기 위한 전자 디지털 컨텐츠 상점(들)(103)을 근거한 위성에 의해 또한 이용되고 있다. 웹 서비스를 통해 배포되는 SC(s)는 방송 서비스를 통해 배포하는 방법과 동일하다.

X. 엔드-유저 장치(들)(109)

안전한 디지털 컨텐츠 전자 배포 시스템(100)용 엔드-유저 장치(들)(109)내에서의 애플리케이션은 두 개의 주 기능-첫째로, SC(s) 처리 및 카피 제어, 둘째로, 암호화 컨텐츠(113)의 플레이백-을 수행한다. 엔드-유저 장치(109)이 퍼스널 컴퓨터나 특정한 전자 고객용 장치라도, 이러한 기본 기능을 수행할 수 있을 것이다. 엔드-유저 장치(들)(109)는 또한 재생 리스트의 생성, 디지털 컨텐츠 라이브러리의 관리, 컨텐츠 플레이백하는 동안의 정보 및 이미지의 디스플레이, 외부 미디어 장치들로의 기록과 같은 다양한 추가 특징 및 기능을 제공한다. 이러한 기능들은 서비스에 따라 차이를 두고, 또한, 애플리케이션은 디자인되는 장치의 타입을 지지한다.

A. 개요

1. 텔레커뮤니케이션 인프라를 통해 전송

도 10은 주요 구성 부분 및 처리가 도시되고, 엔드-유저 장치(들)(109)의 기능 플로우이다. 웹 인터페이스 컨텐츠(113)를 근거한 PC를 지원하기 위해 디자인된 애플리케이션은 두 개의 실행 가능한 소프트웨어 애플리케이션-SC(s) 프로세서(192)와 재생기 애플리케이션(195)으로 구성되어 있다. SC(s) 프로세서(192)는 SC(s) 파일/MIME 타입들을 조정하기 위해 엔드-유저(들) 웹 브라우저(191)로의 헬퍼 애플리케이션으로 구성되어 있는 실행 가능한 애플리케이션이다. 이 애플리케이션은 전자 디지털 컨텐츠 상점(들)(103), 결제소(들)(105) 및 컨텐츠 호스팅 사이트(들)(111)로부터 SC(s)가 수신될 때마다 브라우

저에 의해 실행되기 시작한다. 이것은 SC(s)의 모든 필요 처리를 수행하는데 응답하여, 결국 엔드-유저(들)의 디지털 컨텐츠 라이브러리(196)에 컨텐츠(113)를 추가한다.

재생기 애플리케이션(195)은 그의 디지털 컨텐츠 라이브러리(196)내에서 컨텐츠(113)를 수행하고, 그의 디지털 컨텐츠 라이브러리(196)를 관리하며, 허용된다면 컨텐츠(113)의 복사본을 생성하도록 엔드-유저(들)가 수행하는 단독 실행 가능한 애플리케이션으로 되어 있다. 재생기 애플리케이션(195) 및 SC(s) 처리기(192) 양자는 자바, C/C++ 또는 이와 동등한 소프트웨어로 작성된다. 바람직한 실시예에 있어서, 애플리케이션은 웹 사이트와 같은 컴퓨터가 판독 가능 수단으로부터 다운로드될 수 있다. 그러나, 다른 적당 메커니즘들은 디스켓 또는 CD와 같은 컴퓨터가 판독 가능한 매체 상으로 전달될 가능성이 또한 있어야 한다.

컨텐츠(113) 정보를 검색 및 브라우징은, 예컨대 노래 클립을, 및 구매용 선택 노래를 사전 검토하는 것은 엔드-유저(들) 웹 브라우저(191)를 통해 모두 조정된다. 전자 디지털 컨텐츠 상점(들)(103)은 오늘날 많은 컨텐츠(113) 소매 웹 사이트에 의해 제공되는 동일한 방법으로 쇼핑 경험을 제공한다. 오늘날의 컨텐츠(113) 쇼핑을 경유한 엔드-유저(들)과의 차이점은 그들의 쇼핑 카트에 추가될 다운로드 가능한 컨텐츠(113) 객체들을 자신들이 즉각 선택할 수 있다는 것이다. 전자 디지털 컨텐츠 상점(들)(103)이 다운로드 가능한 객체들에 부가하여 판매에 유용한 다른 상품들을 소유하면, 엔드-유저(들)는 그들의 쇼핑 카트 내에 물리적, 전자적으로 다운로드 가능한 상품의 조합들을 가질 수도 있다. 안전한 디지털 컨텐츠 전자 배포 엔드-유저 장치(들)(109)는 엔드-유저(들)가 체크 아웃하여 전자 디지털 컨텐츠 상점(들)(103)에 그들의 구매 인증서를 제출할 때까지 연관되지는 않는다. 이러한 점 이전에, 모든 상호작용은 전자 디지털 컨텐츠 상점(들)(103)용 웹 서버와 엔드-유저 장치(들)(109)상의 브라우저(191) 간의 것이다. 이것은 디지털 컨텐츠 클립들의 샘플의 미리 보기를 포함한다. 이 디지털 컨텐츠 클립들은 SC(s)로 패키징되지는 않지만, 대신에 다운로드 가능한 파일들로서 전자 디지털 컨텐츠 상점(들)의 웹 서비스로 통합되거나 스트리밍 서버로부터 공급된다. 컨텐츠(13) 클립의 포맷은 시스템 구조에 의해 지시받지는 않는다. 또다른 실시예에 있어서, 재생기 애플리케이션(195)은 전자 디지털 컨텐츠 상점(들)(103) 또는 결제소(들)(105), 또는 오프라인 상에서 판촉 CD와 직접 상호 작용할 수 있다.

2. 컴퓨터로 읽을 수 있는 매체를 통한 전송

이와 다른 실시예에서, 전화선,케이블 TV,다이렉트 TV(direct TV),인터넷과 다른 유선과 무선 통신 하부구조와 같은 통신 라인(line)를 통한 컨텐츠(Content)(113) 또는 재생기 애플리케이션(Player Application) 자체의 다운로딩 대신에, 이 실시예에서는 컴퓨터로 읽을수있는 매체에 관해서 기술되어있다. 컴퓨터로 읽을수 있는 매체는 플로피 디스켓, CDS, DVDS, 포터블 플레쉬 메모리(Portable Flash Memory), 집드라이브(ZipDrives™), 이동 하드 드라이브와 컴퓨터가 정보를 읽을 수 있는 다른 이동매체를 포함한다. 간략화하여, 이 실시예에서 컴퓨터로 읽을 수 있는 매체는 CD(1802)이고 컨텐츠(113)은 음악이다. CD(1802)는 컨텐츠 호스팅 싸이트(Content Hosting Sites)(111)를 대신하여 음악이 광대역과 같은 전자 수단을 통하기보다는 물리적인 매체를 통하여 배포되는 것을 가능하게한다. CD(1802)는 음악 샘플과 다중 압축되고 암호화된 음악 트랙을 컨텐츠 SC안에, 그리고 컨텐츠(113)에관한 관련된 메타데이터(Metadata)를 포함한다. 오디오 세션(audio session)의 샘플 트랙은 표준 CD 재생기에서 재생되어질 수 있다. 엔드 유저 장치(들)(End User Device(s))의 CD 드라이브에 마운트(mount) 되었을때(109)는 자동으로 엔드 유저(end-user)가 음악을 듣고 하나 혹은 그 이상의 압축되고 암호화된 노래를 구입을 위하여 선택하는 것을 가능하게하는 웹브라우저(Web Browser)(191)을 시작한다.

전체의 구매 트랜잭션(transaction) 공정은 컨텐츠 호스팅 싸이트(111)로부터 컨텐츠(113)의 다운로드를 위해서 기술된 대에 사용된 것과 같다. 차이는 부호화된 컨텐츠(113)은 컨텐츠 호스팅 싸이트(111)로부터 다운로드 되지않고 컨텐츠(113)이 CD(1802)에 저장된 컨텐츠 SC(s)(630)에서 읽혀진다는 점에 있다. 따라서, CD(1802)의 사용은 협소한 대역의 인터넷을 통한 긴 다운로드 시간과 광대역 인터넷 채널에 대한 필요성을 없애준다. 전술된 바와 같이, 컨텐츠(113)의 통신 배포를 위하여, 엔드 유지 장치(들)(109)를 사용하는 엔드 유저는 암호화 키(Key)(623)에 엑세스(access)하여 전자 디지털 컨텐츠 상점(Electronic Digital Content Store(s))(103)으로부터 트랜젝션 SC(s)(Transaction SC(s))(641)의 접수에 의하여 컨텐츠(113)을 행한다. 다른 실시예에서 변형된 트랜젝션 SC(s)(1832)가 컨텐츠 공급자(Content Provider 101 또는 결제소(ClearingHouse(s))(101) 또는 처리 거래 인증을 위한 어떠한 다른 제 3의 소스(source)로 부터 접수된다.

CD(1802)에 맞추어질 수 있는 압축되고 암호화된 노래의 수는 오디오 세션의 음악 샘플의 재생시간과 수와 압축된 음악 데이터율과 각 노래의 길이에 의존한다. 예를 들면, 만약 약 20초 가량의 음악 샘플이 허락된다면, 256 kilobit/sec로 압축된 60분 길이의 약 4 음악 작품 또는 128 kilobit/sec로 압축된 8개의 60분 길이의 앨범이 CD(1802)에 맞추어 질 것이다. 만약 컴퓨터로 읽을 수있는 매체가 CD(1802) 대신에 DVD라면, 현재의 DVD 기술은 CD 매체를 통한 압축된 음악 작품의 수의 약 5배 가량을 저장한다. 따라서 현재의 DVD 기술로 256 kilobit/sec로 압축된 20개의 60분짜리 음악작품과 128 kilobit/sec로 압축된 40개의 60분짜리 앨범을 저장하는 것이 가능하다.

CD(1802)에 저장된 정보에 대한 한 실시예가 이제 기술된다. 판촉 패키지(Promotional Package)(1801)라고도 알려진 정보가 (i)본 예에서 오디오 컨텐츠인 컨텐츠 세션 영역(1804) 와 (ii)재생기 애플리케이션(195)의 기능으로 묶여진 데이터 세션(1806)로 알려진 두개의 일반적인 영역으로 분해된다.

컨텐츠 세션 영역(1804)는 다음을 포함한다.

- CD(1802)의 내용에 관한 그리고 하나의 포함된 압축된 노래와 노래들을 구입하기위한 과정에 관한 정보를 가진 정보 오디오 트랙(1808).

- 약 20개의 30초 판촉 음악의 오디오 트랙(1820).

데이터 세션(1806)은 다음을 포함한다.

- 엔드 유저 장치(들)(109)에서 데이터 세션을 시작하는 프로그램 오토런.이섹스이(Autorun.exe) 프로그

램. 만약에 마이크로 소프트 윈도우의 자동실행 기능이 가능하다면, CD와 오토런.이섹스이(autorun.exe)가 자동적으로 실행된다. 그렇지않다면, 엔드 유저 장치(들)(109)는 수동으로 오토런.이섹스이(autorun.exe)(1812)를 시작하여야 한다. CD(1802)의 리드미.텍스트(readme.txt) 파일은(보여지지 않음) 이경우 자동실행기능이 가능하지 않을때 엔드 유저를 안내하는 정보를 가지고 있다. 실행의 한 부분으로써, 오토런.이섹스이(autorun.exe)(1812)는 CD(1802)의 HTML 페이지(1816)의 첫번째 HTML 페이지를 여는데, 이것은 교대로 웹브라우저(191)을 시작하고, 웹브라우저(191)은 자동적으로 첫번째 HTML 페이지가 열리고 이것을 현재의 기준 드라이브로 사용하는 논리적인 드라이브 식별자를 등록한다.

- CD(1802)의 HTML 페이지(1816)의 첫번째 페이지를 가리키는 오토런.아이엔아이(Autorun.ini)(1814) 파일.

- 윈도우에서의 자동실행기능이 가능하지 않을때 엔드 유저를 안내하여 오토런.이엑스이(autorun.exe)(1812) 프로그램을 시작하도록하는 명령을 가진 리드미.티엑스티(Readme.txt) 파일. 이 텍스트 파일은 또한 CD(1802)와 음악 구매 과정을 목적으로하는 정보를 제공한다.

- 엔드 유저가 엔드 유저 장치(들)(109)의 재생기 애플리케이션(Player Application)(195)를 설치하는것을 가능하게하는 재생기 애플리케이션 설치 패키지(Player Application Installation Package)(1818).

- 엔드유저의 검색을 지원하여 음악을 선택하고 엔드유저의 신용카드정보를 수집하여 전자 디지털 컨텐츠 상점(103)에 보내는 일련의 HTML 페이지(1816).

- 각 압축된 앨범의 데이터 세트(data set).

- 컨텐츠 SC(s)(630)과 관련 메타데이터.

- 컨텐츠 SC(s)(630)과 CD(1802)의 트랙 파일을 지시하는 제의 SC(s)(641). 컨텐츠 SC(s)(630)과 트랙 파일은 고정된 디렉토리 구조에 기초한 CD(1802)내에 위치한다.

- 변형된 트랜잭션 SC(s)(1824)는 통신 실시예에서의 트랜잭션 SC(s)(640)과 유사하며 변형된 트랜잭션 SC(s)(1824)는 CD(1802)의 제의 SC(s)(641)을 지시하는 식별자와 이용가능한 사용조건(519)를 포함한다. 변형된 트랜잭션 SC(s)(1824)는 컨텐츠 제공자(101)의 디지털 서명(624)로 디지털적으로 서명될것이다.

도 19도는 본 발명에 따른 디지털 컨텐츠의 권리 획득에대한 도 18의 다른 실시예의 흐름도를 나타낸다. 위 과정은 엔드유저가 CD(1802)를 엔드유저 장치(들)(109)로 로딩하는 단계(1902)로 시작된다. (1904)단계에서, 엔드유저는 정보오디오 트랙과 음악 샘플과 다른 멀티미디어 판촉물을 플롯 수있다. 엔드유저는 CD(1802) 로부터 읽어들인 HTML 페이지와 상호작용을 하는데, 엔드유저는 그/그녀가 구입하고자하는 음악을 선택하고 신용카드 정보를 제공한다. HTML 페이지(1816)은 통신 실시예에서의 제의 SC(s)(640)에서 행해진것과 같이 엔드유저에게 가격과 사용조건(519)를 제공한다.

일단 엔드유저가 구입할 앨범을 선택하고 신용카드정보를 제공하면, 웹브라우저(191)상에서 실행되는 브라우저 스트립트(script) 프로그램은 CD(1802)로부터 전달되고 전자 디지털 컨텐츠 상점(들)(103)과 같은 지불 싸이트로 전송된 통지 SC(s)(1822)을 전달한다. SSL 연결과 같은 안전한 연결이 엔드유저 장치(들)(109)와 지불 싸이트 간에 사용되어 신용카드와 선택 정보를 인터넷에서의 도청으로부터 보호한다.

지불인증을 이룬후에, 변형된 트랜잭션 SC(s)(1824)는 웹 브라우저(191)에의해서 수신된다. 이 변형된 트랜잭션 SC(s)(1824)는 정규의 변형된 트랜잭션 SC(s)(640)과 유사하지만, 제의 SC(s)(641)을 운반하지않고 통지 SC(s)(1822)를 포함한다. 즉, (1908)단계에서, 변형된 트랜잭션 SC(s)(1824)는 트랜잭션 데이터(642),통지 SC(s)(1822)와 음악에대한 사용조건(519)를 운반한다.

재생 애플리케이션(195)는 CD(1802)로부터 선택된 음악에 대한 제의 SC(s)(641)을 수신한다. 그다음에 (1910)단계에서, 위 애플리케이션은 결제소(들)(105)와 정규의 상호작용을 수행하여 통신 실시예에 대하여 도 6에서 이미 기술한 바와 같이 선택된 컨텐츠(113)에 대한 라이센스 SC(s)(660)을 획득한다.

컨텐츠(113)에 대한 라이센스 SC(s)(660)이 수신된 후에, 재생기 애플리케이션(195)는 CD(1802)로부터 해당하는 컨텐츠 SC(s)(630)을 복사하고 도 6에 대한 통신 실시예에서 기술된 이 부분들의 정규의 처리를 수행한다.

CD(1802)에 대한 컨텐츠 준비는 위 섹션 VIII에서 기술된 바와 같은 시스템과 기법이다. 그러나 통신 네트워크를 통한 배포를 위한 컨텐츠 SC(s)(630)을 생성하는 대신에, 컨텐츠 SC(s)(630)과 제의 SC(s)(640)은 CD(1802)에 씌여진다. 각각의 노래에 대한 통지 SC(s)(1822)와 각각의 노래를 위한 제공 SC(s)와 일련의 HTML 페이지(1816)은 CD(1802)에 포함된다. 오토런.이엑스이(autorun.exe)(1812)와 오토런.아이엔아이(autorun.ini)(1814)와 엔드유저 애플리케이션 설치 패키지(1818)은 CD(1802)에 포함될것이다.

이 컴퓨터로 읽을수있는 매체의 배포 실시예뿐만아니라 컨텐츠(113) 전달의 통신 실시예를 지원하기 위하여 재생기 애플리케이션(195)에 필요한 변화는 아래의 "섹션 X.D 재생기 애플리케이션"에 나열된 모든 구성요소를 포함한다.이것은 두 전달 실시예 모두에 양립하게 만든다. 부가적으로, 재생기 애플리케이션 설치 패키지(1818)의 기능은 다음 소프트웨어를 포함한다.

- 엔드유저가 CD(1802)에 포함된 앨범을 선택하는 것을 가능하게 한다.

- 엔드유저가 제의 SC(s)(641)의 위치와 컨텐츠 SC(s)(630)을 지시하는 것을 가능하게 한다. 만약 필요한 제공 SC(s)(641)이 CD(1802)에서 이용할수 없을때에는 HTML 주소가 전자 디지털 컨텐츠 상점(들)(103)에 제공된다.

- 제공 SC(s)(641), 디지털 서명(641)과 이용가능한 사용조건(519)에 해당하는 식별자를 포함하는 통지 SC(s)(1822)를 생성한다.

- 음악의 선택과 구입에 있어서 엔드유저를 안내할 HTML 페이지의 생성을 가능하게 한다. 위 HTML 페이지 생성은 페이지 템플릿(template)에 기초를 둘것이다. 위 템플릿은 음악에 관한 정보를 포함할 수있는 HTML 페이지(1816)의 생성과 맞춤을 가능하게 하여야한다. 각 노래에대한 정보는 자켓(Jacket)과 커버 아트(cover art)와 가사와 사용조건을 포함할수있다. 템플릿은 엔드유저에게 주어져 신용카드 정보를 수집하는 HTML 형식의 생성과 맞춤을 가능하게 한다.

- 오퍼레이터(operator)가 오토런.이엑스이(autorun.exe)(1812), 오토런.아이엔아이(autorun.ini)(1814) 파일과 위 재생기 애플리케이션 셀치 패키지(1818)의 위치를 지시하는것을 가능하게 한다.

- HTML 페이지(1816)의 첫번째 HTML 페이지 를 지시하기위해서 엔드유저가 오토런.아이엔아이(autorun.ini)(1814) 파일을 변형하는것을 가능하게 한다.

- 엔드유저가 오디오 정보와 음악 샘플 트랙을 선택하는것과 온라인(online) URLS를 지시하는것을 가능하게 한다.

지금까지 기술된 것은 CD(1802)를 통한 컨텐츠 전달이다. CD상에 판촉 암호화된 컨텐츠는 정규의 음악 또는 DVD CD의 일부가 될수있음에 주의하여야 한다. 위 CD(1802)는 섹션D "재생기 애플리케이션"아래의 서브섹션(sub-section) 4 "암호해독(1505), 압축해제(1506)과 재생기 요소(1506)"에서의 공정에 의하여 생성되어질 수있다. 위 CD(1802)는 컨텐츠 제공자(들)(101) 또는 전자 디지털 컨텐츠 상점(들)(103)으로부터의 판촉 패키지(1801)를 포함한다. 이 CD(1802)가 재생되면 유저 혹은 유저의 친구가 매우 빨리 CD(1802)의 컨텐츠(113)에대한 권리를 구입하는것을 가능하게한다. 즉, 만약 유저가 듀기위해서 CD(1802)를 친구집에 가져간다면, 친구는 컨텐츠 호스팅 싸이트(들)(111)로부터 컨텐츠(113)을 다운로드 받지않고서 자신만의 이용을위한 CD(1802)의 복사본을 만들 권리를 구입할 수있다. 이것은 친구들과 동료사이에 판촉용 패키지(1801)의 빠른 전파를 가능하게 한다. 인터넷상의 상점 또는 다운로딩 컨텐츠(113)으로 돌아가기보다는 친구가 도 19아래에서 기술된 공정 흐름을 사용하여 CD(1802)에 암호화된 컨텐츠(113)의 복사본을 생성할 수있다. 컨텐츠(113)외에, 재생기 애플리케이션(195) 또한 CD(1802)에 전송되어서 공중을 통한 재생기 애플리케이션(195)의 빠른 전파가 가능할 수있다.

다른 실시예에서, 판촉용 패키지(1801)은 엔드유저간에 이메일(E-mail)될수있다. 오늘날 전화선을 통한 압축된 파일의 전송이 여전히 느리지만, 케이블모뎀과 같은 좀더 고속의 네트워크는 용량을 증가시킬 것이다. 유저에게 판촉 패키지(1801)를 다른 사람에게 이메일할 수있는 능력을 부여함으로써, 컨텐츠(113)은 이메일 목록의 어떤 사람에 의해서도 구입되어질 수있다.

B. 애플리케이션 설치

재생기 애플리케이션(195)와 헬퍼 애플리케이션(1981)은 많은 웹싸이트나 섹션 X.A.3 컴퓨터로 읽을 수있는 매체를 통한 전달에서의 위 실시예를 통해서 입수가능한 자기설치 수행가능한 프로그램으로 패키지되어진다. 결제소(들)(105)는 공공 웹 싸이트에서 주다운로드 페이지를 주관하는 중심 위치로 동작한다. 이것은 설치 패키지가 다운로드되어질 수있는 위 위치로의 연결을 포함한다. 설치 패키지는 모든 컨텐츠 호스팅 싸이트(들)(111)에서 입수가능하여 다운로드 요구의 지리적 분산을 제공한다. 각각의 참여하고있는 전자 디지털 컨텐츠 상점(들)(103)은 또한 위 패키지가 그들의 싸이트로부터 다운로드하여 입수가능하게 하거나 위 결제소(들)(105)의 공공 웹 싸이트의 주 다운로드 페이지로의 연결을 제공할것이다.

다운로드가능한 컨텐츠(113)을 구입하고자하는 엔드유저(들)은 이 패키지를 다운로드받아서 설치한다. 위 설치는 이 다운로드할수있는 패키지에 자기 포함되어있다. 이것은 헬퍼 애플리케이션(198)과 재생기 애플리케이션(195) 모두를 풀어서 설치하고 또한 헬퍼 애플리케이션(198)을 설치된 웹 브라우저(들)에 형성한다.

설치의 일부분으로써, 공공/개인 키(Key)(661) 쌍은 주문과 라이센스 SC(s)(660) 과정에서의 사용을위한 엔드유저 장치(들)을 위하여 생성된다. 임의의 대칭키(비밀 유저 키) 또한 라이센스 데이터베이스(197)에서 노래 암호화 키를 보호하는데 이용하기 위하여 생성된다. 위 비밀유저키(나타나지않음)는 키를 여러부분으로 나누어서 키조각을 엔드유저의 컴퓨터를 통해서 여러 위치에 저장함에의해서 보호된다. 위 코드의 이 영역은 위 키가 어떻게 분할되며 어디에 저장되는지 누설하지 않기 위하여 탬퍼 레지스턴트 소프트웨어(Tamper Resistant Software) 기법으로 보호된다. 심지어 엔드유저(들)에 의한 이 키로의 접근을 방지하는것은 프라이버시나 컨텐츠(113)의 다른 컴퓨터와의 공유를 방지하는것을 돕는다. 이들 키가 어떻게 이용되는지에 대한 좀더 상세한 설명을 위하여 위 SC(s) 프로세서(192) 섹션을보라.

탬퍼 리시스턴트 소프트웨어 기법은 해커에의한 컴퓨터 소프트웨어 애플리케이션으로의 인증받지않은 진입을 방지하기위한 방법의 하나이다. 전형적으로 위 해커는 위 소프트웨어를 이해하여 그리고/또는 변형하여 사용에대한 제한을 제거하기를 원한다. 실제적으로, 해킹을 당하지않을 수있는 컴퓨터 프로그램은 존재하지않는다; 이것이 탬퍼 리지스턴트 소프트웨어가 템퍼푸루프(tamper-proof)라고 불리지않는 이유이다. 그러나 탬퍼 리지스턴트 보호 애플리케이션을 해킹하는데 필요로하는 노력의 양은 위 노력이 가능한 이익의 가치가 없기때문에 대체로 대부분의 해커를 방지한다. 여기서 위 노력은 컨텐트(113)의 한조각의, 아마 CD안의 노래한곡의, 키로의 접근을 얻게될것이다.

탬퍼 리지스턴트 소프트웨어기법의 한 종류는 IBM으로부터이다. 이 코드가 도입된 한 생산물은 IBM ThinkPad 770 랩탑(laptop) 컴퓨터이다. 여기서 탬퍼 리지스턴트 소프트웨어는 컴퓨터내의 DVD 영화 재생기를 보호하는데 사용되었다. 헐리우드 스튜디오와 같은 디지털 컨텐츠 제공자는 디지털 영화의 출현과 완전한 복사본이 만들어질 수있는 용이함을 걱정하며 복사 방지 메카니즘(mechanism)을 포함하는 DVD 디스크의 영화를 요구하였다. IBM의 탬퍼 리지스턴트 소프트웨어는 이 복사 방지 메카니즘을 회피하는것을 어렵게 만들었다. 이것은 전형적인 탬퍼 리지스턴트 소프트웨어의 응용이다: 위 소프트웨어는 컨텐츠(113)의 몇몇 보호된 형태의 사용에대한 규칙을 강화하는데 이용된다.

IBM의 탬퍼 리지스턴트 소프트웨어는 다수의 형태의 장애물을 공격자의 통로에 놓는다. 먼저, 이것은 해커가 사용하는 표준 소프트웨어 툴인 디버거(debugger)와 디스어셈블러(disassembler)의 효과를 물리치거나 혹은 최소한 좁이는 기법을 포함한다. 두번째로 이것은 셀프 인테그리티 체킹(self-integrity

checking)를 포함하여 하나의 변조 혹은 심지어 아주작은 변조라도 감지되어서 올바르지않은 동작을 야기시킨다. 마지막으로, 이것은 혼란(obfuscation)을 포함하여 해커가 진정한 동작으로 여기도록 그릇되게 인도한다. 뒤의 기법은 대개 임시적이지만 앞의 두 기법은 암호서기법에서 잘 알려진 툴인 암호화와 디지털 서명에의해 만들어졌다.

C. 안전한 컨테이너 프로세서(192)

엔드유저가 그가 그의 쇼핑 카트안에 수집한 상품에대한 마지막 구입 인증을 전자 디지털 컨텐츠 상점(들)(103)에 제출할 때에, 그의 웹브라우저는 웹서버로부터 응답을 기다리며 활동중인 상태로 남는다. 전자 디지털 컨텐츠 상점(들)(103)의 위 웹서버는 구입을 처리하며 재정적인 해결을 수행하며 그리고나서 엔드유저 장치(들)(109)에 트랜잭션 SC(s)를 돌려보낸다. SC(s) 프로세서(192)(헬퍼 애플리케이션(198))은 위 웹 브라우저에의해서 개시되어 트랜잭션 SC(s)(640)과 관련한 SC(s) 마임(mime)형을 처리한다. 도 14는 본 발명에 따라 도 10에서 기술된 로컬 라이브러리(local library)로의 재생기 애플리케이션(195) 다운로딩 컨텐츠의 유저 인터페이스 스트린(user interface screen)의 한 예이다.

위 SC(s) 프로세서(192)는 트랜잭션 SC(s)(640)을 열고 안에있는 반응 HTML 페이지와 제공 SC(s)(641)를 추출한다. 반응 HTML 페이지는 엔드유저의 구매를 나타내는 브라우저 윈도우에 나타난다. (1401)단계에서 제공 SC(s)(641)은 그다음에 열려지며 투영된 다운로드 시간에 따른 컨텐츠(113)(예를 들면 노래나 앨범) 이름이 그들로부터 추출된다. (1402)단계에서 이 정보를 가진 새로운 윈도우가 그다음에 나타나며, 엔드유저(들)에게 컨텐츠(113)(예를들면 음악,노래 또는 전체 앨범에 대한)의 다운로드 예정이 선택사항으로 주어진다. 엔드유저(들)은 즉각적인 다운로드를 선택하거나 다운로드를 예정하여 나중에 할수 있다. 만약 다른 시간이 선택된다면, 다운로드 예정정보는 로그(log)에 저장되고 만약 엔드유저 장치(들)(109)가 그 시간에 전원이 켜져있다면, 다운로드는 예정된 시간에 시작된다. 만약 위 컴퓨터가 예정된 시간에 동작하지 않거나 통신 링크(link)가 동작하지 않는다면, 엔드유저(들)은 다음에 컴퓨터에 전원이 들어오게되면 다운로드를 다시 예정한다.

예정된 다운로드 시간이 발생하거나 즉각적인 다운로드가 요청된다면, 위 SC(s) 프로세서(192)는 위 트랜잭션 SC(s)(640), 제의 SC(s)(641),그리고 설치시간에 생성된 엔드유저(들)의 공공 키(661) 에있는 정보로부터 주문 SC(s)(650)을 생성한다. 이 주문 SC(s)(650)은 HTTP 요청을 경유하여 결제소(들)(105)로 보내어진다. 위 결제소(들)(105)가 위 라이센스 SC(s)가 돌려보냈을때, 위 헬퍼 애플리케이션(198)은 재자극되어 위 라이센스 SC(s)(660)을 처리한다. 다음에 라이센스 SC(s)(660)은 열려지며 컨텐츠 호스팅 싸이트(들)(111)의 URL이 위 기준된 주문 SC(s)(650)으로부터 추출된다. 다음에 라이센스 SC(s)(660)은 브라우저를 통한 http 요청을 경유하여 컨텐츠 SC(s)(630)의 다운로드를 요청하는 위 특정된 컨텐츠 호스팅 싸이트(111)로 보내진다. 컨텐츠 SC(s)(630)이 브라우저로 돌아오면 헬퍼 애플리케이션(198)은 다시 재자극되어진다. 위 SC(s) 프로세서(192)는 다운로드 진행 지시자와 완성 추정시간을따라서 다운로드된 컨텐츠(113)의 이를을 나타낸다.

위 SC(s) 프로세서(192)에 의해서 컨텐츠(113)이 수신될 때, 컨텐츠(113) 데이터는 암호해독을 위해서 메모리 버퍼로 로딩된다. 버퍼의 크기는 암호 알고리즘과 워터마킹(watermarking) 기법(193)의 필요량에 의존하며, 해커 코드에 노출된 비암호화 컨텐츠(113)의 양을 줄일수있는 최소의 크기이다. 버퍼가 채워짐에 따라, 라이센스 SC(s)(660)으로부터 추출된 엔드유저(들)의 위 키(623)(공공키(661)에 해당하는)를 이용하여 암호해독되는데 이것자체는 처음으로 사설키를 사용하여 암호해독되어지는 것이다. 암호해독된 버퍼는 다음에 워터마킹 기능으로 넘겨진다.

워터마킹(193)은 라이센스 SC(660)로부터 워터마킹 인스트럭션을 추출해내고 엔드 유저(들)의 개인 키를 사용하여 인스트럭션을 암호해독한다. 이후에 전자 디지털 컨텐츠 상점(들)(103)이 등록 기능을 제공하지 않는다면, 이 컨텐츠(113)가 구입되어진 전자 디지털 컨텐츠 상점(103)에 등록되거나 또는 신용 카드 등록 정보로부터 획득된(derived from) 구매자 이름과 같은 트랜잭션 정보를 포함하는 라이센스 SC(660)로부터 워터마킹 데이터가 추출된다. 또한 이 트랜적션을 위해 로깅된 특정 기록을 참조하기 위해 전자 디지털 컨텐츠 상점(103)에 의해 부여된 구매 데이터 및 트랜잭션 ID(535)가 워터마크에 포함된다. 상점 사용 조건(519)이 재생기 애플리케이션의 카피 제어(195)에 또한 포함된다.

워터마킹(193)은 워터마킹 인스트럭션의 출처를 밝히지 않도록 함으로써 해커가 워터마크의 위치 및 기술을 발견하는 것을 방지하는 위조 방지 코드(Tamper Resistant Code) 기술에 의해 보호된다. 이것은 해커에 의한 워터마크의 제거 또는 변경을 방지한다.

컨텐츠 버퍼에 임의로 요청된 워터마크를 등록한 이후에, 버퍼는 재암호화(194)를 위해 스크램블링 기능(scrambling function)에 패스된다. IBM사의 봉인(IBM'S SEAL) 암호화 기술과 같은 효율적인 안전한 암호화 프로세서가 랜덤 대칭 키(a random Symmetric Key)를 사용하여 컨텐츠(113)를 재암호화하는데 사용된다. 다운로드 및 암호해독 및 재암호화(194) 프로세스가 일단 완성되면, 처음부터 컨텐츠(113)를 암호화하기 위해 컨텐츠 제공자(101)에 의해 사용된 암호화 키(623)가 이제 파괴되고 새로운 봉인 키(SEAL key)가 설치 기간때에 생성되고 은신된 비밀 사용자 키(Secret User Key)를 사용하여 스스로 암호화된다. 이 새로운 암호화 봉인 키가 이제 라이센스 데이터베이스(107)에 저장된다.

컨텐츠 제공자(들)(101)에서 수행된 다른 소스 및 엔드 유저 장치(들)(109)에서 수행된 사용자 워터마킹은 산업 표준안으로서 유효하게될 필요가 있다. 이들 표준은 여전히 전개되고 있다. 이 기술은 제어 정보가 음악에 내장되고 여러차례 갱신되도록 하는데 효율적이다. 그러한 회수가 카피 제어 표준안(the copy control standards)에서와 같이 좀 더 안정화될 때까지, 다른 카피 제어 방법이 안정한 디지털 컨텐츠 전자 배분 시스템(100)에 제공되며 그것은 소비자 장치에 권리 관리를 제공하기 위해 카피 제어 워터마크에 종속되지 않는다. 저장 및 재생/기록 사용 조건 안전성은 엔드 유저 장치(들)(109)에 결합되고 위조 방지 환경을 통해 보호되는 암호화된 DC 라이브러리 집합체(196)를 이용하여 구현된다. 표준안(standards)이 채택되어 졌을 때 소프트웨어 훅(software hooks)이 적절한 장소에 위치하여 카피 제어 워터마킹를 지원한다. 지원(supports)은 오늘날 워터마킹 AAC 및 기타 다양한 압축 레벨에 인코딩된 오디오 스트림을 위해 존재하지만 이 기술이 현재 단독의 카피 제어방법으로서 사용하기에는 여전히 약간 미완성적이다.

암호해독 및 재암호화(194) 프로세스는 원컨텐츠(the original content:113) 암호화 키, 새로운 봉인 키, 비밀 유저 키 및 비밀 유저 키 세그먼트가 저장되는 곳 및 키가 세스먼트되는 방법이 누설되지 않도록 하는 위조 방지 코드 기술에 의해 보호되는 또 다른 코드 영역이다.

암호화 및 재암호화(194) 프로세스는 두가지 목적을 제공한다. 봉인과 같은 알고리즘으로 암호화된 컨텐츠(113)를 저장하는 것은 실시간 암호화보다 보다 빠르게 이네이블하게 하고 암호해독을 수행하는 처리 이용률 또한 데스(DES)와 같은 산업 표준 타입에 좀 더 가까운 것에 의해 수행되는 것 보다 매우 적게 요구한다. 이것은 재생기 애플리케이션(195)이 디코드 및 재생에 우선하여 컨텐츠(113)를 위한 전체 파일을 먼저 암호화할 필요 없이 컨텐츠(113)의 실시간 동시 암호해독-디코딩-재생을 수행하는 것을 이네이블하게 한다. 봉인 알고리즘 및 고 효율의 디코딩 알로리즘의 효율성은 동시 기능(암호화된 파일로부터 재생녹음을 스트리밍함)을 허용하는 것이 아니라 이 프로세스가 매우 낮은 파워 시스템 프로세서에서도 발생할 수 있도록 허용한다. 그러므로 이 애플리케이션은 60MHz 펜티엄 시스템 및 혹은 이보다 낮은 로우엔드(low end)와 같은 엔드 유저 장치(들)(109)상에 지원될 수 있다. 원암호화 포맷(the original format)으로부터 최종적으로 저장되는 컨텐츠(113)에서 암호화 포맷을 구별한다는 것은 원컨텐츠 암호화 알로리즘의 선택에 있어서 보다 큰 융통성을 발휘한다. 그러므로 산업 표준 알로리즘에 의해 넓게 수용되고 입증된 사용은 안전한 디지털 컨텐츠 전자 배분 시스템(100)의 디지털 컨텐츠 산업 승인(Digital Content Industry acceptance)를 더욱 강화시키는데 사용될 수 있다.

암호해독 및 재암호화(194) 프로세스의 제 2 목적은 이 컨텐츠(113)를 암호화하기 위해, 컨텐츠 제공자(들)(101)에 의해 사용된 원마스터 암호화 키(the original master encryption Key:623)가 이 컨텐츠를 라이센싱하는 모든 엔드-유저 장치(들)(109)상에 저장되어야 한다는 요건을 제거하는데 있다. 라이센스 SC(들)(600)의 일부로서 암호화된 마스터 키(623)는 단지 매우 짧은 시간동안 엔드 유저 장치(들)(109)의 하드 디스크상에서만 캐쉬(cached)되거나 매우 짧은시간 동안 메모리에서만 암호해독(in the clear)된다. 이 실행 단계(execution phase)동안, 키(623)는 위조 방지 코드 기술을 통해 보호된다. 이 키(623)가 엔드 유저 장치(들)(109)에서 임의의 형태로 유지될 필요는 없지만 이 암호해독 및 재암호화(194) 단계가 완성되면, 해커로부터의 표절(piracy)의 가능성이 작아진다.

일단 노래가 재암호화되면, 그것은 디지털 컨텐츠 라이브러리(196)에 저장된다. 재생기 애플리케이션(195)에 의한 사용에 따라 요청된 모든 메타데이터는 관련 제의 SC(들)(641)로부터 추출되거나 또는 디지털 컨텐츠 라이브러리(196)에서 저장된다(단계 1403). 노래 가사와 같은 암호화되는 임의의 메타데이터 일부는 기타 다른 컨텐츠에서 설명된 바와 동일한 방식으로 암호해독되고 재암호화된다. 컨텐츠(113)를 암호화시키는데 사용된 동일한 봉인 키는 암호화될 필요가 있는 임의의 관련 메타데이터를 위해 사용된다.

D. 재생기 애플리케이션(195)

1. 개요

안전한 디지털 컨텐츠 전자 배분 재생기 애플리케이션(195)(본 명세서에서는 재생기 애플리케이션(195)으로서 지칭됨)은 CD, DVD 또는 기타 다른 디지털 컨텐츠 재생기 및 CD, DVD 또는 기타 다른 디지털 컨텐츠 저장 관리 시스템과 유사하다. 가장 단순하게, 그것은 노래 또는 비디오 재생과 같은 컨텐츠(113)를 수행한다. 또 다른 레벨에서, 그것은 그/그녀의 디지털 컨텐츠 라이브러리(196)을 관리하는 엔드 유저(들)를 제공한다. 그리고 중요한 것은, 그것은 예를 들면 노래(본명세서에서 재생-리스트로 지칭됨)와 같은 컨텐츠의 집합체를 편집(editing)하고 재생하는 것을 제공한다는 것이다.

재생기 애플리케이션(195)은 컨텐츠 제공자(들)(101) 및 전자 디지털 컨텐츠 상점(들)(103)의 요구에 개별적으로 선택되거나 또는 커스텀화될 수 있는 구성요소의 집합체로부터 조립된다. 포괄적 재생기 버전이 기술되지만 커스텀화가 가능하다.

이제 도 15를 참조하면, 도 10의 엔드 유저 장치(들)(109)상에서 실행하는 주 구성요소 및 재생기 애플리케이션(195)의 프로세스 블럭도가 도시된다.

재생기 객체 관리자(1501)의 서브시스템을 구성하는 다양한 구성요소-세트로는

1. 엔드 유저 인터페이스 구성요소(1509)
2. 카피/재생 관리 구성요소(1504)
3. 암호해독(1505), 압축해제(1506), 재생 구성요소(1507) 및 기록을 포함할 수 있음
4. 데이터 관리(1502) 및 라이브러리 액세스 구성요소(1503)
5. 애플리케이션 간 통신 구성요소(1508)
6. 기타 (설치 등) 구성요소

가 존재한다.

각각의 이들 세트내의 구성요소들은

- 플랫폼(윈도우, 유닉스 또는 이와 등가물)
- 통신 프로토콜(네트워크, 케이블 등)
- 컨텐츠 제공자(들)(101) 또는 전자 디지털 컨텐츠 상점(들)(103)
- 하드웨어(CD,DVD 등)
- 결제소(들)(105) 기술 그 이상

의 요건에 기초하여 선택된다.

후술될 부분들은 다양한 구성요소 세트들을 기술한다. 최종 부분에서는 이들 구성요소가 어떠한 방법으로 포괄적 재생기에서 구성되는지를 기술하며 이 구성요소가 어떠한 방식으로 커스텀화될 지를 논의한다.

또 다른 실시예에서, 재생기 애플리케이션(195) 및 SC 프로세서(192)의 구성요소는 프로그래머의 소프트웨어 툴킷(toolkit)의 일부로써 사용가능하다. 이 툴킷은 위에서 리스트된 포괄적 재생기 애플리케이션의 구성요소와의 사전정의된 인터페이스를 이네이블하게 한다. 이들 사전정의된 인터페이스는 API 또는 애플리케이션 프로그래밍 인터페이스 형태로 존재한다. 이들 API를 사용한 개발자는 고 레벨의 애플리케이션 프로그램으로부터 구성요소의 임의의 기능성을 구현할 수 있다. 이들 구성요소에 API를 제공함으로써, 프로그래머는 이들의 기능 및 이들의 임의의 구성요소 자원을 재생산할 필요 없이 커스텀화된 재생기 애플리케이션(195)을 신속히 전개시킬 수 있다.

2. 엔드 유저 인터페이스 구성요소(1509)

이들 세트로부터의 구성요소들이 결합하여 재생기 애플리케이션(195)의 스크린상 표시(on-screen manifestation)를 제공한다. 디자인은 이들 구성요소의 최종적인 레이아웃도 설정되지 않았다는 것에 유의하여야 한다. 그러한 레이아웃은 포괄적 재생기에 제공된다. 컨텐츠 제공자(들)(101) 및/또는 전자 디지털 컨텐츠 상점(들)로부터의 요건 및 기타 다른 요건에 기초하여, 다른 레이아웃이 가능하다.

이들 세트는 엔드 유저 디스플레이(1510)를 제공하는데 사용된 구성요소로부터 개시하는 서브그룹들로 그룹화되고 처리(handle)는 오디오 재생 및 메타 데이터의 제시와 같은 저 레벨 기능에 사용되는 소위 엔드 유저 제어(1511)를 제어한다. 다음으로, 엔드 유저 디스플레이 구성요소(1510)는 특정 기능 그룹화(재생 리스트, 디지털 컨텐츠 라이브러리) 및 이후에 이들 저 레벨 구성요소의 그룹화 및 배치에 사용된 객체 컨테이너 구성요소에 의해 또한 분리된다.

후술될 구성요소 리스트 작성(listing)에 있어서, CDS 생성 또는 CD 또는 기타 다른 기록 가능 매체로의 컨텐츠(113) 카피에 대한 임의의 참조는 재생기 애플리케이션(195)이 그러한 이네이블한 가능성을 어디에서 갖는냐의 경우에만 적용될 뿐이다. 또한 문맥(context)이 포괄적인 하나로 존재한다는 점에서 그 용어 CD는 또한 다양한 다른 외부 기록 장치, 예를 들면 미니디스크 또는 DVD 등을 표현할 수 있다는 점에 유의하여야 한다.

도 16은 본 발명에 따른 도 15의 재생기 애플리케이션(195)의 유저 인터페이스 스크린의 실례이다. 엔드 유저 제어(1511)를 위한 기능은

컨텐츠(113)를 수행하는 제어 수단(Controls for performing the Content):

- 재생/정지 버튼
- 재생 버튼
- 정지 버튼
- 일시 중지 버튼
- 순방향 스킵 버튼(Skip forward button)
- 역방향 스킵 버튼(skip backward button)
- 볼륨 조절
- 위치 제어/디스플레이 트랙킹
- 오디오 채널 볼륨 레벨 디스플레이 등.

컨텐츠(113)과 연관된 메타데이터를 디스플레이하는 제어 수단

- 화면 버튼 커버(Cover Picture button)
- 화면 객체 커버
- 아티스트 화면 버튼
- 아티스트 화면 객체
- 리스트 버튼 트랙킹
- 리스트 정보 객체 트랙킹
- 리스트 선택자 객체 트랙킹 (재생용 클릭)
- 이름 객체 트랙킹
- 정보 객체 트랙킹
- 가사 버튼 트랙킹
- 가사 객체 트랙킹
- 아티스트 이름 객체 트랙킹
- 크레디트 버튼 트랙킹(Track Credits button)
- 크레디트 객체 트랙킹

· CD 이름 객체
· CD 크레디트 버튼(CD Credits button)
· CD 크레디트 객체
· 포괄적 (구성가능) 메타데이터 버튼
· 포괄적 데이터 객체 등
을 포함한다(엔드 유저 인터페이스의 대용스크린이 (1601) 내지 (1605)에 도시됨).
엔드 유저 디스플레이(1510)을 위한 기능은
디스플레이 컨테이너의 재생 리스트
· 재생 리스트 관리 버튼
· 재생 리스트 관리 윈도우
· 디지털 컨텐츠 검색 버튼
· 디지털 컨텐츠 검색 제출 버튼
· 디지털 컨텐츠 검색 결과 버튼
· 선택된 검색 결과 아이템을 재생 리스트 버튼에 카피
· 재생 리스트 객체(편집 가능)
· 재생 리스트 저장 버튼
· 재생 리스트 재생 버튼
· 재생 리스트 중지 버튼
· 재생 리스트 재시작 버튼
· 재생 리스트 버튼 등으로부터 CD 생성
디지털 컨텐츠 라이브러리(196)의 디스플레이
· 디지털 컨텐츠 라이브러리 버튼
· 디지털 컨텐츠 라이브러리 관리자 윈도우
· 디지털 컨텐츠 카테고리 객체
· 바이-아티스트 버튼(By-artist button)
· 바이-장르 버튼
· 바이-레이블 버튼
· 바이-카테고리 버튼
· 버튼 삭제
· 부가-대-재생 리스트 버튼(Add-to-Play-list button)
· CD 버튼으로 카피
· 노래 리스트 객체
· 노래 리스트 디스플레이 컨테이너 등
컨테이터 등
· 재생기 윈도우 컨테이너
· 오디오 제어 컨테이너
· 메타데이터 제어 컨테이너
· 메타데이터 디스플레이 컨테이너
· 툴바 컨테이너 객체
· 샘플 버튼
· 다운로드 버튼
· 구매 버튼
· 레코드 버튼
· 재생기 이름 객체
· 라벨/제공자/저장 광고 객체

· 라벨/제공자/저장 URL 버튼

· 아티스트 URL 버튼 등

를 포함한다(엔드 유저 인터페이스의 대응 스크린이 (1601) 내지 (1605)에 도시됨).

3. 카피/재생 관리 구성요소(1504)

이들 구성요소는 암호화 키, 워터마크 처리, 카피 관리 등의 설정(set up)을처리한다. 인터페이스는 또한 지불이 완료되었는지(pay per listen) 또는 컨텐츠(113)로의 각각의 액세스가 어디에서 기인되었는지의 경우와 같은 특정 서비스를 위한 결제소(들)(105)와의 통신, 구입 요청의 전송 등의 경우에 존재한다. 현재, 결제소(들)(105) 기능과의 통신은 SC(s) 프로세서(192)에 의해 처리된다.

엔드 유저 장치(들)(109) 상에서의 재생기 애플리케이션(195)에 의한 컨텐츠(113)의 사용은 라이센스 데이터베이스(197)과 같은 데이터베이스내에서 로깅(logged)된다. 재생기 애플리케이션(195)에 의한 각각의 컨텐츠(113) 사용의 트랙킹은 결제소(들)(105) 또는 컨텐츠 제공자(들)(101) 또는 전자 디지털 컨텐츠 상점(들)(103) 또는 전송 인프라(107)에 결합되고 지시된 임의의 사이트와 같은 하나 이상의 로깅 사이트(logging sites)에 전송될 수 있다. 이 전송은 사용 정보를 로깅 사이트로 업로드하기 위해 사전결정된 시간에서 스케줄되어 질 수 있다. 예상된 하나의 사전결정된 시간은 전송 인프라(107)가 네트워크 트래픽과 혼잡하지 않을 이른 아침일 수 있다. 알려진 기술을 사용한 재생기 애플리케이션(195)은 스케줄된 시간에서 실행(wake up)하며 로컬 로깅 데이터베이스로부터 로깅 사이트로 정보를 전송한다. 로깅 사이트 정보를 검토함으로써, 컨텐츠 제공자(들)(101)은 자신의 컨텐츠(113)의 인기(popularity)를 측정할 수 있다.

또 다른 실시예에서, 이후에 로깅 사이트로 업로딩하기 위한 컨텐츠(113)의 사용을 로깅하는 대신에, 컨텐츠(113)의 사용이 컨텐츠(113)의 매번의 사용 동안 로깅 사이트로 업로딩된다. 예를 들면, DVD 디스크, 디지털 테잎, 플래시 메모리, 미니디스크 또는 이와 등가의 판독/기록 가능한 제거 가능 매체(removable media)와 같은 외부 장치 상에 엔드 유저 장치(들)(109)에 저장된 컨텐츠(113)를 복사(duplicating)하거나 또는 카피할 때, 로깅 사이트에 이 사용이 갱신된다. 이것은 컨텐츠(113)가 구매되었을 때 전송되는 사용자 조건(206)에 컨텐츠(113)를 카피하는것이 필수조건이 될 수 있다. 이것은 컨텐츠 제공자(들)(101)가 컨텐츠(113)상에서 이들의 재생, 복사 또는 기타 다른 동작 동안 이들의 컨텐츠(113) 사용을 정확히 트랙킹할 수 있다는 것을 보장한다.

또한, 이 컨텐츠(113)에 대한 다른 정보가 로깅 사이트에 업로딩될 수 있다. 예를 들면, 최근에(예를 들면 한시간 또는 하루전) 컨텐츠(113)가 수행되었는가, 컨텐츠(113)가 몇번 수행되는가, 컨텐츠(113)가 DVD 디스크, 디지털 테잎 또는 미니-디스크와 같은 인증된 외부 장치에서 복사되거나 또는 카피되는가 이다. 상이한 가족 구성원의 경우 처럼, 엔드 유저 장치(들)(109) 상에 다수의 개별적인 단일 재생기 애플리케이션(195) 사용자가 어디에 존재하느냐의 경우에, 컨텐츠(113) 사용자 식별은 로깅 사이트에서 사용자 정보에 따라 전송된다. 로깅 사이트로 업로드된 사용자 정보를 검토함으로써, 컨텐츠 제공자(들)(101)은 컨텐츠(113)가 수행되어진 실제 사용, 사용자 식별 및 횟수에 기초하여 컨텐츠(113)의 인기를 측정할 수 있다. 실제 사용 측정은 텔레비전, 또는 전화 조사를 위한 닐쉘 순위 기법(a Nielsen Rating scheme)과 같은 샘플링 방법을 사용하며 이 시스템을 좀 더 실제로 시스템상에서 구동되도록 하며, 제한된 사용자 수만이 임의로 한번에 샘플링되어 이 결과가 추정된다. 본 실시예에서, 실제 사용은 전자 디지털 컨텐츠 상점(들)(103) 또는 컨텐츠 제공자(들)(101)과 같은 지시된 웹 사이트로 로깅 백(logging back)하는 사용자들을 위해 측정될 수 있다.

4. 암호해독(1505), 압축해제(1506) 및 재생 구성요소

이 구성요소들은 카피/재생 관리 구성요소에 의해 획득되는 키를 사용하여 데이터 관리 및 라이브러리 액세스 구성요소들로부터 획득되는 오디오 데이터를 언로크(unlock)하고, 재생용 오디오 데이터를 마련하기 위해 적절한 압축해제를 적용하며, 그것을 재생하기 위해 시스템 오디오 서비스를 사용한다. 다른 실시예에서, 데이터 관리 및 라이브러리 액세스 구성요소들로부터 획득되는 오디오 데이터는 CD, 디스켓, 테이프 혹은 미니디스크 등과 같은 삭제가능 매체에 복사될 수 있다.

5. 데이터 관리(1502) 및 라이브러리 액세스 구성요소(1503)

이 구성요소들은 엔드 유저 시스템상의 여러 저장 장치상의 가요 데이터를 저장 및 검색하는 것뿐만 아니라 저장된 가요에 관한 정보에 대한 요구를 처리하는데 사용된다.

6. 애플리케이션 간 통신 구성요소(1508)

이 구성요소들은 안전한 디지털 컨텐츠 전자 배포 재생기와 재생기 애플리케이션(195)을 호출할 수도 있거나 그 재생 애플리케이션(195)이 자신의 기능을 수행할 경우 사용할 필요가 있는 기타 애플리케이션(가령, 브라우저, 헬퍼 애플리케이션 및 플러그인 등) 간의 조정 가능을 위해 사용된다. 가령, URL 제어가 활성화될 경우, 그 URL 제어는 적절한 브라우저를 호출하여 그 브라우저에 적절한 페이지를 로딩하도록 명령한다.

7. 기타 구성요소

전술한 범주(가령, 인스톨)에 포함되지 않는 별도의 구성요소들은 여기에 그룹화된다.

8. 포괄적 재생기

이 부문에서는 재생기 애플리케이션(195)의 버전내로 전술한 구성요소들이 조합되는 것이 논의된다. 이러한 것은 여러 상이한 일예들 중의 하나인데, 그 이유는 재생기 애플리케이션(195)이 소프트웨어 객체에 기초하는 것에 의해 커스텀화용으로 설계되기 때문이다.

재생기 객체 관리자(1501)는 기타 모든 구성요소들을 함께 보유하고 있는 소프트웨어 프레임워크이다. 이전의 부문에서 논의된 바와 같이, 도면의 재생기 객체 관리자(1501) 아래의 블록들은 임의의 재생기용

으로 요구되고 있지만, 사용중에 있는 암호화 혹은 스크램블링의 형태, 오디오 압축 타입, 컨텐츠(113) 라이브러리에 대한 액세스 메쏘드와 같은 것에 의존하는 특정 버전으로 대체될 수도 있다.

재생기 객체 관리자(1501) 위에는 가변 객체(1512)가 있는데, 이들은 대부분 재생중이거나 탐색중인 컨텐츠(113)와 관련한 메타데이터로부터 유도된다. 이렇한 가변 객체들은 엔드 유저 디스플레이(1510)와 엔드 유저 제어(1511)로부터 수신된 입력을 통해 엔드 유저 장치(109)에 이용가능하도록 만들어진다. 모든 객체들은 구성가능(configurable)하며, 모든 컨테이너의 층들은 커스텀가능하다. 이러한 객체들은 C/C++, 자바 혹은 임의의 동등한 프로그래밍 언어로 구현될 수 있다.

(재생기 애플리케이션(195)의 사용)

다음의 실시예는 엔드 유저 장치(109)상에서 실행되는 재생기 애플리케이션(195)이 컨텐츠(113)가 음악으로 되는 오디오 재생기인 일예를 나타내고 있다. 본 기술분야의 숙련가라면 다른 타입의 컨텐츠(113)가 재생기 애플리케이션(195)에 의해 지지될 수 있다는 것을 이해해야 한다. 전형적인 오디오 애호가는 가요를 보유하고 있는 CD 라이브러리를 갖는다. 이러한 모든 것들은 안전한 디지털 컨텐츠 전자 배포 시스템(100)내에서 이용될 수 있다. 전자 디지털 컨텐츠 상점(103)으로부터 구매된 가요 세트는 그 시스템의 디지털 컨텐츠 라이브러리(196)내에 저장된다. 물리적 CD와 유사한 가요의 그룹은 재생 리스트로서 저장된다. 일부에 있어서, 재생 리스트는 정확히 CD를 에뮬레이트한다(가령, 상용 CD의 모든 트랙은 온라인 버전의 CD로서 전자 디지털 컨텐츠 상점(103)으로부터 구매되며, CD의 온라인 버전과 동등한 재생 리스트에 의해 규정되고 있다). 그러나, 대부분의 재생 리스트들은 엔드 유저가 그 시스템상의 디지털 컨텐츠 라이브러리내에 저장한 가요를 그룹화하도록 엔드 유저에 의해 함께 편집된다. 그러나 차후의 논의를 위해, 재생 리스트의 용어가 언급될 경우에 커스텀하게 제조된 음악 CD의 일예가 사용된다.

엔드 유저가 재생기 재생기 애플리케이션(195)를 SC 프로세서(192)로부터의 요청을 통해 개시하기 보다는 직접적으로 개시할 경우, 그 유저는 그것을 액세스된 최종의 재생 리스트로 사전로딩한다. 만약 디지털 컨텐츠 라이브러리(196)내에 재생 리스트가 존재하지 않는다면, (만약 유저가 우선 세팅을 통해 이러한 특징을 턴오프하지 않는다면)재생 리스트 편집기가 자동으로 개시된다. 아래의 세목을 나타내는 재생 리스트를 참조하기 바란다.

재생기 애플리케이션(195)는 또한 인수(argument)로서의 특정 가요를 통해 호출될 수 있는데, 이 경우 재생기 애플리케이션은 즉시 가요 재생 모드로 진입한다. 선택 사양적으로, 가요는 재생을 위해 마련될 수 있지만, 재생 전에 엔드 유저에 의한 동작을 대기한다. 이러한 경우에 보다 상세한 아래의 가요 재생를 참조하기 바란다.

(재생 리스트(엔드 유저 인터페이스(1603)의 해당 스크린))

엔드 유저가 재생 리스트 기능을 호출할 경우 그 재생 리스트의 기능에는 아래의 이용가능한 기능들이 있다. 즉,

* 재생 리스트 개방.

* 선택용으로 저장된 재생 리스트의 리스트를 디스플레이하기 위해 디지털 컨텐츠 라이브러리 호출(보다 상세한 것은 아래의 디지털 컨텐츠 라이브러리를 참조).

* 재생 리스트 편집.

* 사전 로딩된 현재의 재생 리스트가 마련된 재생 리스트 편집기를 호출. 사전 로딩되지 않은 경우 비어있는 그 편집기가 함께 개시하기 위한 재생 리스트를 생성.

* 재생 리스트를 실행.

* 선택된 가요(혹은 가요가 선택되지 않은 경우 재생 리스트의 개시 가요)로 시작되는 가요들을 한번에 한번씩 재생. 재생 리스트 편집기내의 옵션 세트는 재생의 순서에 영향을 끼친다. 그러나 재생 리스트의 재생을 위한 옵션들을 오버라이드하는데 제어가 이용될 수 있다.

* 가요 재생.

* 재생 리스트로부터 선택된 가요만을 재생. 보다 많은 정보를 위해 아래의 가요 재생를 참조.

* 재생 리스트 정보.

* 재생 리스트에 관한 정보를 디스플레이.

* 가요 정보.

* 재생 리스트 내의 선택된 가요에 관한 정보를 디스플레이.

* 웹 싸이트 방문.

* 이 재생 리스트와 관련한 웹 싸이트를 브라우저내로 로딩.

* 라이브러리.

* 디지털 컨텐츠 라이브러리 윈도우를 개방. 또한 보다 많은 정보를 위해 아래의 디지털 컨텐츠 라이브러리를 참조.

(재생 리스트 편집기(엔드 유저 인터페이스(1603)의 해당 스크린))

재생 리스트 편집기를 호출할 경우 엔드 유저 옵션에는 다음과 같은 것이 있다. 즉,

* 재생 리스트 보기(view)/로딩/삭제.

* 하나를 선택하기 위해 저장된 재생 리스트의 리스트를 디스플레이하여 로딩하거나 삭제하도록 디지털

컨텐츠 라이브러리를 호출. 보다 상세한 정보를 위해서는 아래의 디지털 컨텐츠 라이브러리를 참조.

* 재생 리스트를 저장.

* 현재의 버전의 재생 리스트를 디지털 컨텐츠 라이브러리(196)에 저장.

* 가요 삭제.

* 재생 리스트로부터 현재 선택된 가요를 삭제.

* 가요 추가

* 재생 리스트에 추가하기 위한 가요를 선택하기 위해 디지털 컨텐츠 라이브러리를 가요 탐색 모드에서 호출. 보다 상세한 정보를 위해 아래의 디지털 컨텐츠 라이브러리를 참조.

* 가요 정보를 세트.

* 재생 리스트내의 선택된 가요에 관한 정보를 디스플레이하여 변경. 이 정보는 재생 리스트에 저장되지만, 디지털 컨텐츠 라이브러리(196)내에 저장된 가요에 관한 정보를 변경시키지는 않는다. 이러한 것들은 변경될 수 있다.

* 디스플레이된 가요 타이틀.

* 가요에 관한 엔드 유저 노트.

* 가요 재생시 리드인(lead-in) 지연.

* 가요 재생 후의 팔로우온 지연(follow-on delay).

* 재생시 가요 내의 개시 포인트.

* 재생시 가요 내의 종료 포인트.

* 랜덤 모드를 위한 가중화.

* 이러한 가요 등을 위한 볼륨 조정.

(재생 리스트 속성 세트: 이 재생 리스트의 속성을 디스플레이하여 변경. 이 속성은 다음과 같이 세트될 수 있음)

* 재생 리스트 타이틀.

* 재생 리스트 모드(랜덤, 순차 등)

* 반복 모드(한번 재생, 완료시 재시작 등)

* 이 재생 리스트에 관한 엔드 유저 노트.

(라이브러리(엔드 유저 인터페이스(1601)의 해당 스크린))

* 디지털 컨텐츠 라이브러리 윈도우를 개방. 보다 상세한 정보를 위해 아래의 디지털 컨텐츠 라이브러리를 참조.

(가요 재생)

인자로서의 가요와 함께 재생 애플리케이션(195)를 호출하거나 혹은 재생 리스트로부터 혹은 디지털 컨텐츠 라이브러리 내에서의 재생 가요를 선택함으로써 가요가 재생될 준비가 되었을 경우, 다음과 같은 엔드 유저 옵션이 존재한다(엔드 유저 인터페이스(1601)의 해당 스크린).

* 재생.

* 일시멈춤.

* 정지.

* 역방향 스킵.

* 순방향 스킵.

* 볼륨 조절.

* 트랙 위치 조정.

* 가사 보기.

* 크레디트(credits) 보기.

* CD 커버 보기.

* 아티스트 픽쳐 보기.

* 트랙 정보 보기.

* 기타 메타데이터 보기.

* 웹 싸이트 방문.

* 재생 리스트.

* 라이브러리 등.

(디지털 컨텐츠 라이브러리)

디지털 컨텐츠 라이브러리는 가요 혹은 재생 리스트를 선택할 때 묵시적으로 호출될 수 있거나, 혹은 엔드 유저 시스템 상의 가요 라이브러리의 관리를 위해 자신의 윈도우에서 개방될 수 있다. 그러한 경우 다음과 같은 엔드 유저 옵션이 존재한다.

* 가요 작업;

-아티스트, 범주, 라벨, 등의 모든 것을 소트.

-아티스트, 범주, 라벨, 등에 의한 가요를 선택.

-현재의 재생 리스트에 선택된 가요를 추가.

-(가능한 경우)CD에 가요를 카피.

-가요 삭제.

-범주 등에 가요를 추가.

*재생 리스트 작업;

-이름에 의한 소트.

-범주에 의한 소트.

-선택된 재생 리스트 로딩.

-재생 리스트 재명명.

재생 리스트 삭제.

-키워드에 의한 탐색.

-(가능한 경우)선택된 재생 리스트로부터 CD 생성.

본 발명의 특정 실시예가 개시되었지만, 본 기술분야의 숙련가라면 본 발명의 사상과 범위내에서 이 특정 실시예에 임의의 변경을 가할 수 있음을 이해해야 할 것이다. 본 발명의 범위는 이 특정 실시예에 국한되는 것이 아니며, 첨부되는 특허청구범위가 본 발명의 범위내의 모든 응용예, 변경예, 및 실시예를 커버하고 있음을 이해해야 할 것이다.

발명의 효과

본 발명에 따르면, CD 및 DVD 와 같은 컴퓨터 판독가능 매체 상에서 그리고 인터넷 및 월드와이드웹(WWW)과 같은 글로벌 통신 네트워크 상에서 인쇄 매체, 영화, 게임 및 음악과 같은 디지털 자산(digital assets)의 안전한 전달(secure delivery) 및 이 디지털 자산에 대한 권리 관리를 위한 시스템 및 관련 툴을 제공할 수 있다.

(57) 청구의 범위

청구항 1. 암호화된 디지털 컨텐츠를 컨텐츠 재생 시스템으로 전달하는 방법에 있어서,

이전에 상기 컨텐츠와 연관되어 있는 메타데이터를 컴퓨터 판독가능 매체로부터 판독하는 단계와,

상기 메타데이터로부터 암호해독할 연관된 컨텐츠를 선택하는 단계와,

상기 컨텐츠를 암호해독하기 위해 인증국과 안전한 접속을 확립하는 단계와,

허가된 대로 컴퓨터 판독가능 매체상에 저장된 기암호화된 컨텐츠의 적어도 일부를 암호해독하기 위한 암호해독 키를 수신하는 단계를 포함하는

암호화된 디지털 컨텐츠를 컨텐츠 재생 시스템으로 전달하는 방법.

청구항 2. 제 1 항에 있어서,

상기 암호해독 키를 통해 상기 암호화된 컨텐츠를 암호해독함으로써 기암호화된 컨텐츠의 적어도 일부를 재생하는 단계를 더 포함하는

암호화된 디지털 컨텐츠를 컨텐츠 재생 시스템으로 전달하는 방법.

청구항 3. 제 2 항에 있어서,

상기 암호해독 단계는 상기 암호해독 키에 대해 허가되지 않은 액세스를 방지하기 위해 부정조작되기 어려운 환경에서 행해지는

암호화된 디지털 컨텐츠를 컨텐츠 재생 시스템으로 전달하는 방법.

청구항 4. 제 1 항에 있어서,

상기 암호해독 단계는

허가된 대로 기암호화된 컨텐츠의 적어도 일부를 암호해독하는 단계와,

고유의 로컬 암호해독 키를 사용하여 상기 암호해독된 컨텐츠를 재암호화하는 단계와,

상기 컨텐츠를 라이브러리에 저장하는 단계와,

상기 고유의 로컬 암호해독 키를 사용하여 상기 라이브러리로부터 상기 컨텐츠의 적어도 일부를 암호해독하는 단계를 더 포함하는

암호화된 디지털 컨텐츠를 컨텐츠 재생 시스템으로 전달하는 방법.

청구항 5. 제 4 항에 있어서,

상기 암호해독 및 재암호화 단계는 상기 암호해독 키에 대해 허가되지 않은 액세스를 방지하기 위해 부정 조작되기 어려운 환경에서 행해지는

암호화된 디지털 컨텐츠를 컨텐츠 재생 시스템으로 전달하는 방법.

청구항 6. 암호화된 디지털 컨텐츠를 컨텐츠를 재생하기 위한 엔드 유저 시스템에 전달하기 위한 방법에 있어서,

이전에 상기 컨텐츠와 연관되어 있는 메타데이터를 컴퓨터 판독가능 매체로부터 판독하는 단계와,

상기 메타데이터로부터 암호해독할 연관된 컨텐츠를 선택하는 단계와,

상기 컨텐츠를 암호해독하기 위해 인증국과 안전한 접속을 확립하는 단계와,

허가된 대로 기암호화된 컨텐츠의 적어도 일부를 암호해독하기 위한 암호해독 키를 포함하고 있는 안전한 컨테이너를 수신하는 단계와,

결제소로부터의 암호화 키를 사용하여 안전한 컨테이너를 생성하는 단계-상기 안전한 컨테이너는 상기 엔드 유저 시스템으로부터의 암호화 키를 내장하고 있음-와,

상기 컨텐츠를 암호해독하는 허가의 인증을 위해 상기 결제소로 상기 안전한 컨테이너를 전송하는 단계와,

허가된 대로 컴퓨터 판독가능 매체 상에 저장된 기암호화된 컨텐츠의 적어도 일부를 암호해독하기 위한 상기 암호해독 키를 포함하며, 상기 엔드 유저 시스템의 상기 암호화 키를 사용하며 암호화된 안전한 컨테이너를 상기 결제소로부터 수신하는 단계와,

상기 엔드 유저 시스템의 상기 암호화 키를 사용하여 상기 안전한 컨테이너를 암호해독하여 상기 암호화된 컨텐츠의 적어도 일부를 암호해독하는 상기 암호해독 키에 액세스함으로써 상기 기암호화된 컨텐츠의 적어도 일부를 재생하는 단계를 포함하는

암호화된 디지털 컨텐츠를 컨텐츠를 재생하기 위한 엔드 유저 시스템에 전달하기 위한 방법.

청구항 7. 제 6 항에 있어서,

상기 재생 단계는 다수의 개별 타이틀을 포함하고 있는 기암호화된 컨텐츠의 적어도 일부를 재생하는 단계를 더 포함하며, 이를 통해 각각의 개별 타이틀은 고유 암호해독 키를 통해 암호해독되는

암호화된 디지털 컨텐츠를 컨텐츠를 재생하기 위한 엔드 유저 시스템에 전달하기 위한 방법.

청구항 8. 제 6 항에 있어서,

상기 확립 단계는 상기 인증국에 크레디트 정보를 전송하는 단계를 더 포함하는

암호화된 디지털 컨텐츠를 컨텐츠를 재생하기 위한 엔드 유저 시스템에 전달하기 위한 방법.

청구항 9. 제 6 항에 있어서,

비암호화된 컨텐츠를 포함하고 있는 CD 혹은 DVD 상에 판촉 패키지의 일부로서 인스트럭션을 저장하고 있는

암호화된 디지털 컨텐츠를 컨텐츠를 재생하기 위한 엔드 유저 시스템에 전달하기 위한 방법.

청구항 10. 암호화된 디지털 컨텐츠를 시스템에 전달하기 위한 컴퓨터 판독가능 매체에 있어서,

이전에 상기 컨텐츠와 연관되어 있는 메타데이터를 컴퓨터 판독가능 매체로부터 판독하기 위한 인스트럭션과,

상기 메타데이터로부터 암호해독할 연관된 컨텐츠를 선택하기 위한 인스트럭션과,

상기 컨텐츠를 암호해독하기 위해 인증국과 안전한 접속을 확립하기 위한 인스트럭션과,

허가된 대로 컴퓨터 판독가능 매체상에 저장된 기암호화된 컨텐츠의 적어도 일부를 암호해독하기 위한 암호해독 키를 수신하기 위한 인스트럭션을 포함하는

암호화된 디지털 컨텐츠를 시스템에 전달하기 위한 컴퓨터 판독가능 매체.

청구항 11. 제 10 항에 있어서,

암호해독 키를 통해 암호화된 컨텐츠를 암호해독함으로써 기암호화된 컨텐츠의 적어도 일부를 재생하기 위한 인스트럭션을 더 포함하는

암호화된 디지털 컨텐츠를 시스템에 전달하기 위한 컴퓨터 판독가능 매체.

청구항 12. 제 10 항에 있어서,

상기 암호해독 인스트럭션은 상기 암호해독 키에 대해 허가되지 않은 액세스를 방지하기 위해 부정조작되기 어려운 환경에서 행해지는

암호화된 디지털 컨텐츠를 시스템에 전달하기 위한 컴퓨터 판독가능 매체.

청구항 13. 제 10 항에 있어서,

상기 암호해독 인스트럭션은

허가된 대로 기암호화된 컨텐츠의 적어도 일부를 암호해독하기 위한 인스트럭션과,

고유의 로컬 암호해독 키를 사용하여 상기 암호해독된 컨텐츠를 재암호화하기 위한 인스트럭션과,

상기 컨텐츠를 라이브러리에 저장하기 위한 인스트럭션과,

상기 고유의 로컬 암호해독 키를 사용하여 상기 라이브러리로부터 상기 컨텐츠의 적어도 일부를 암호해독하기 위한 인스트럭션을 더 포함하는

암호화된 디지털 컨텐츠를 시스템에 전달하기 위한 컴퓨터 판독가능 매체.

청구항 14. 제 13 항에 있어서,

상기 암호해독 및 재암호화를 위한 인스트럭션은 상기 암호해독 키에 대해 허가되지 않은 액세스를 방지하기 위해 부정조작되기 어려운 환경에서 행해지는

암호화된 디지털 컨텐츠를 시스템에 전달하기 위한 컴퓨터 판독가능 매체.

청구항 15. 암호화된 디지털 컨텐츠를 엔드 유저 시스템에 전달하기 위한 컴퓨터 판독가능 매체에 있어서,

이전에 상기 컨텐츠와 연관되어 있는 메타데이터를 컴퓨터 판독가능 매체로부터 판독하는 인스트럭션 단계와,

상기 메타데이터로부터 암호해독할 연관된 컨텐츠를 선택하는 인스트럭션 단계와,

상기 컨텐츠를 암호해독하기 위해 인증국과 안전한 접속을 확립하는 인스트럭션 단계와,

허가된 대로 기암호화된 컨텐츠의 적어도 일부를 암호해독하기 위한 암호해독 키를 포함하고 있는 안전한 컨테이너를 수신하는 인스트럭션 단계와,

결제소로부터의 암호화 키를 사용하여 안전한 컨테이너를 생성하는 인스트럭션 단계-상기 안전한 컨테이너는 상기 엔드 유저 시스템으로부터의 암호화 키를 내장하고 있음-와,

상기 컨텐츠를 암호해독하는 허가의 인증을 위해 상기 결제소로 상기 안전한 컨테이너를 전송하는 인스트럭션 단계와,

허가된 대로 컴퓨터 판독가능 매체 상에 저장된 기암호화된 컨텐츠의 적어도 일부를 암호해독하기 위한 상기 암호해독 키를 포함하며, 상기 엔드 유저 시스템의 상기 암호화 키를 사용하여 암호화된 안전한 컨테이너를 상기 결제소로부터 수신하는 인스트럭션 단계와,

상기 엔드 유저 시스템의 상기 암호화 키를 사용하여 상기 안전한 컨테이너를 암호해독하여 상기 암호화된 컨텐츠의 적어도 일부를 암호해독하는 상기 암호해독 키에 액세스함으로써 상기 기암호화된 컨텐츠의 적어도 일부를 재생하는 인스트럭션 단계를 포함하는

암호화된 디지털 컨텐츠를 엔드 유저 시스템에 전달하기 위한 컴퓨터 판독가능 매체.

청구항 16. 제 15 항에 있어서,

상기 재생 인스트럭션 단계는 다수의 개별 타이틀을 포함하고 있는 기암호화된 컨텐츠의 적어도 일부를 재생하는 인스트럭션 단계를 더 포함하며, 이를 통해 각각의 개별 타이틀은 고유 암호해독 키를 통해 암호해독되는

암호화된 디지털 컨텐츠를 엔드 유저 시스템에 전달하기 위한 컴퓨터 판독가능 매체.

청구항 17. 제 15 항에 있어서,

상기 안전한 접속을 확립하는 인스트럭션 단계는 상기 인증국에 크레디트 정보를 전송하는 인스트럭션 단계를 포함하는

암호화된 디지털 컨텐츠를 엔드 유저 시스템에 전달하기 위한 컴퓨터 판독가능 매체.

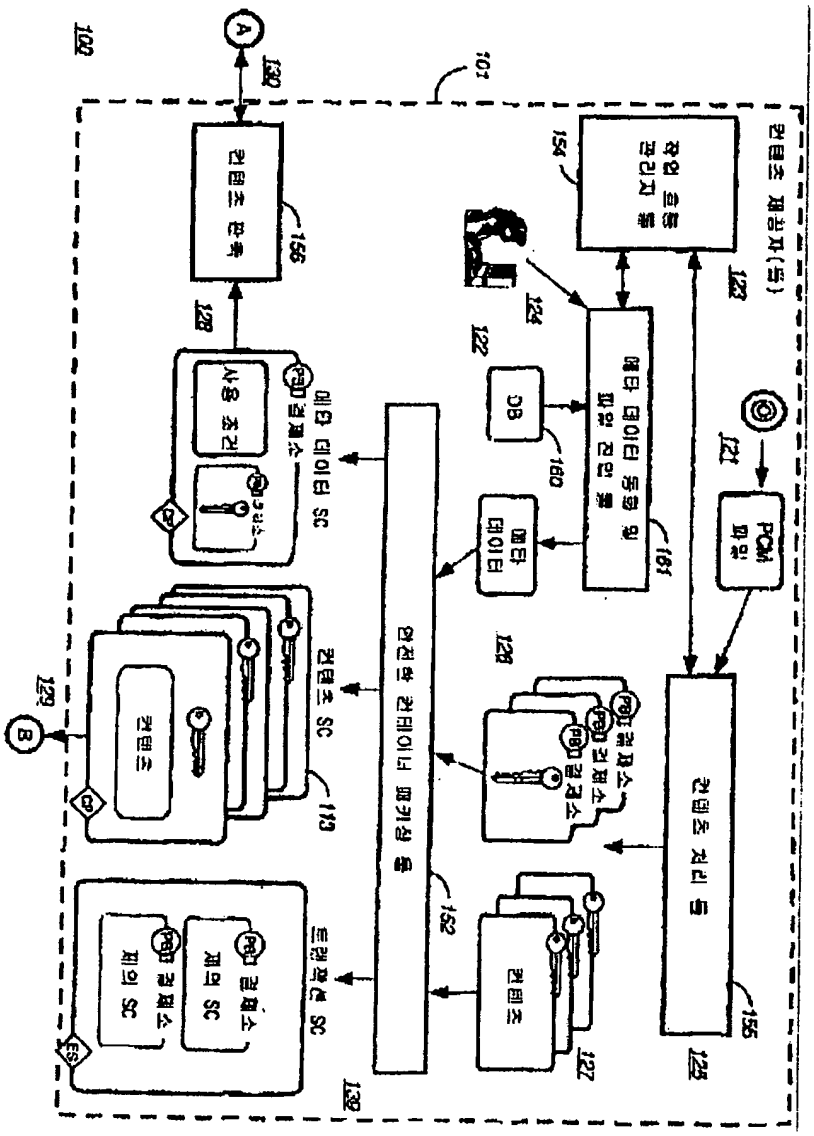
청구항 18. 제 15 항에 있어서,

상기 인스트럭션들은 비암호화된 컨텐츠를 포함하고 있는 CD 혹은 DVD 상에 판촉 패키지의 일부로서 저장되는

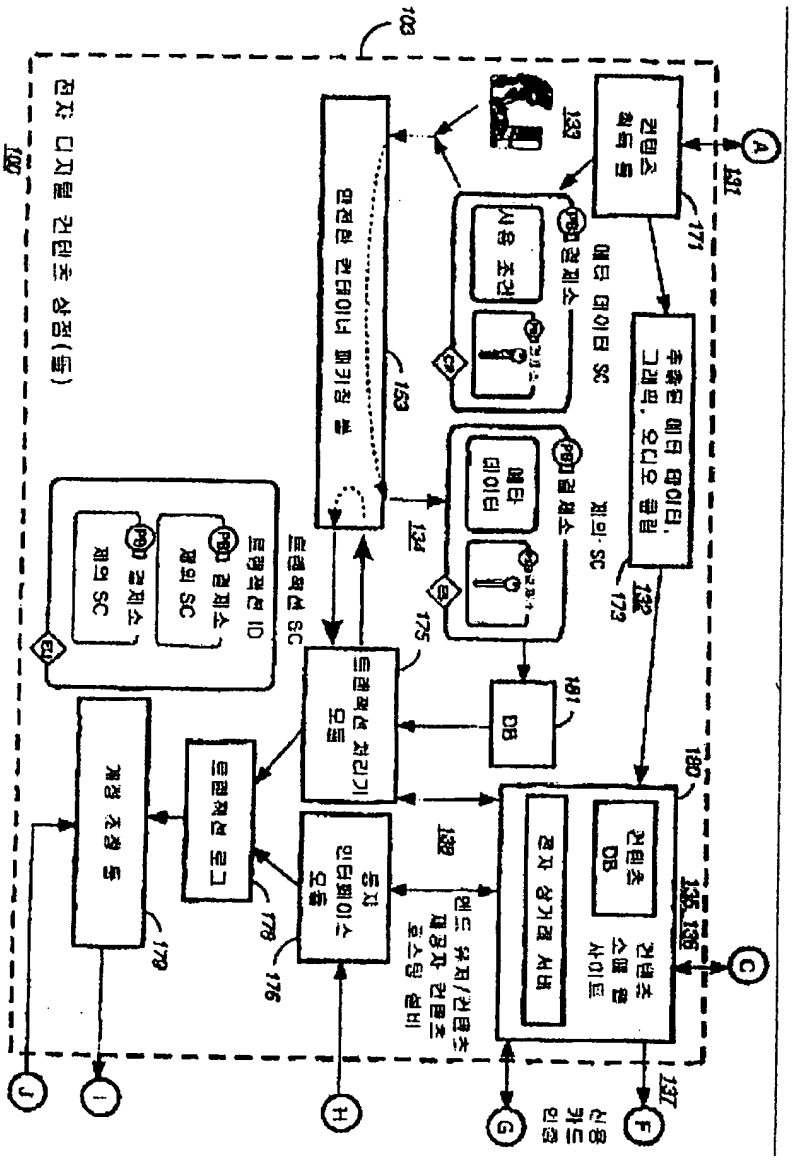
암호화된 디지털 컨텐츠를 엔드 유저 시스템에 전달하기 위한 컴퓨터 판독가능 매체.

도면

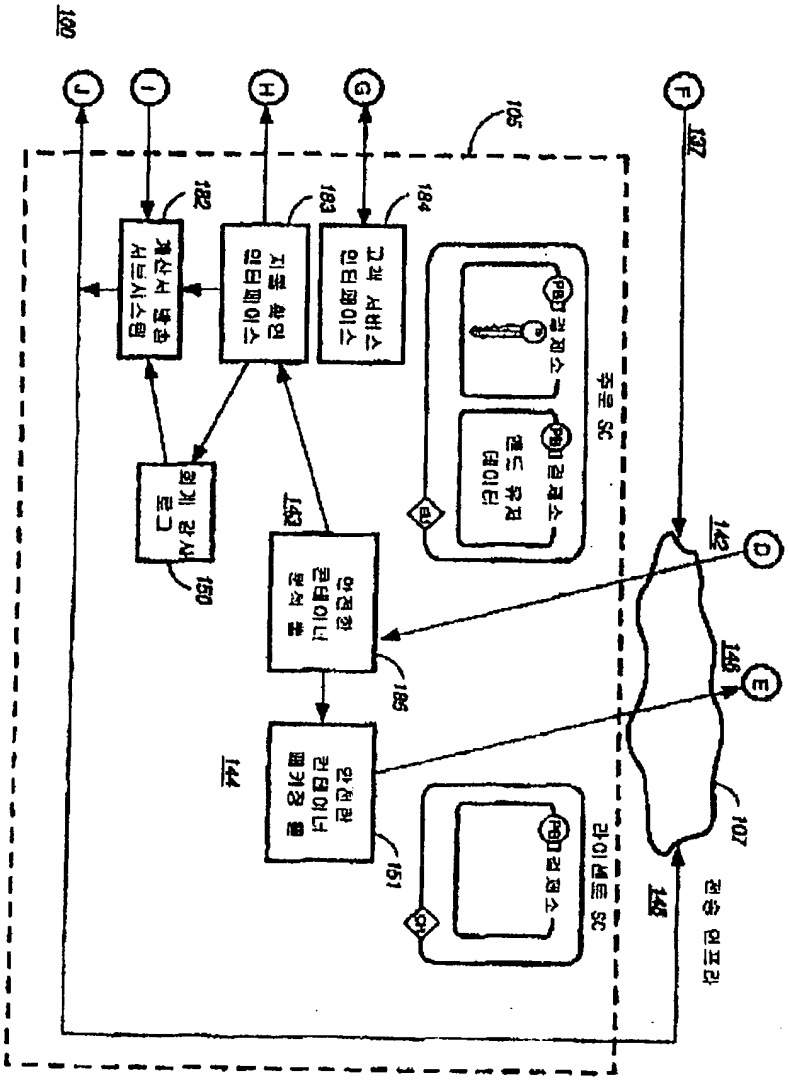
도면1a


컨테이너 재공지(등)
작업 순서 관리자 툴
컨테이너 관리
사용 조건
메타 데이터 SC
컨테이너 SC
컨테이너
트랜잭션 SC
패키 SC
패키 SC
DB
메타 데이터 동등 및 패키 관리 툴
메타 데이터
PDM 파일
안전한 컨테이너 패키징 툴
컨테이너 처리 툴
컨테이너
결제수
결제수
결제수
결제수
결제수
A
B
100
101
121
122
123
124
125
126
127
128
129
130
132
152
154
155
156
160
161

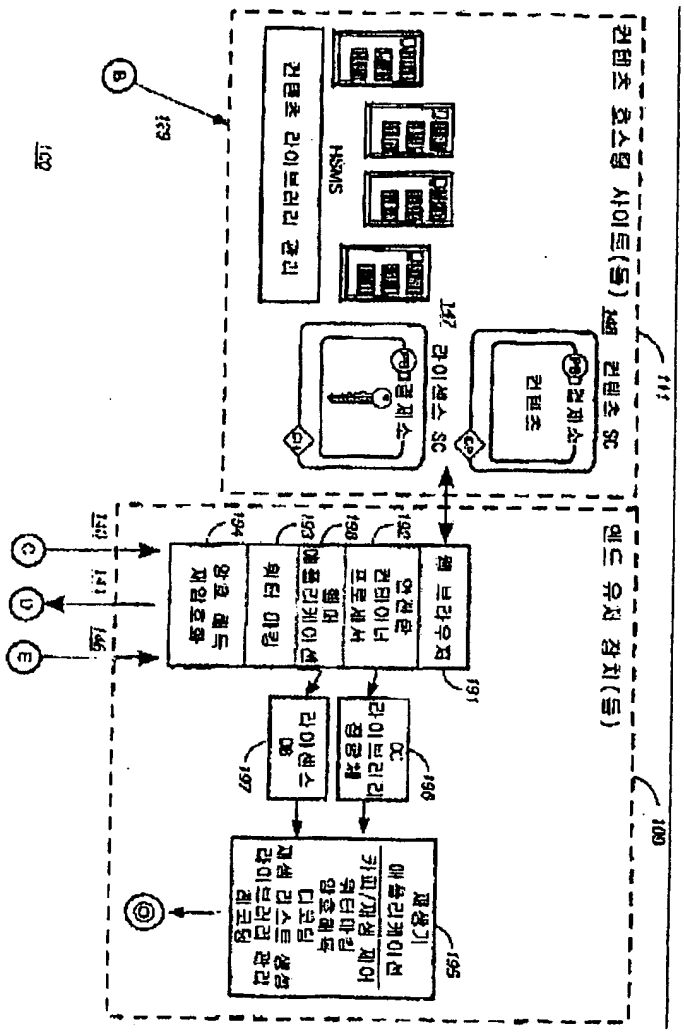
도면16


100
전자 디지털 컨텐츠 상점(들)
101
131
컨텐츠 획득 툴
133
171
메타 데이터 SC
사용 조건
메타 데이터
제1 SC
132
172
제1 컨텐츠
제2 SC
제2 컨텐츠
트랜잭션 ID
트랜잭션 SC
153
패키징 툴
124
125
트랜잭션 처리기 모듈
DB
161
180
컨텐츠 DB
135
136
컨텐츠 등록 사이트
137
신용 카드 인증
138
보안 인터페이스 모듈
176
트랜잭션 로그
178
계정 조정 툴
179
A
C
F
G
H
I
J

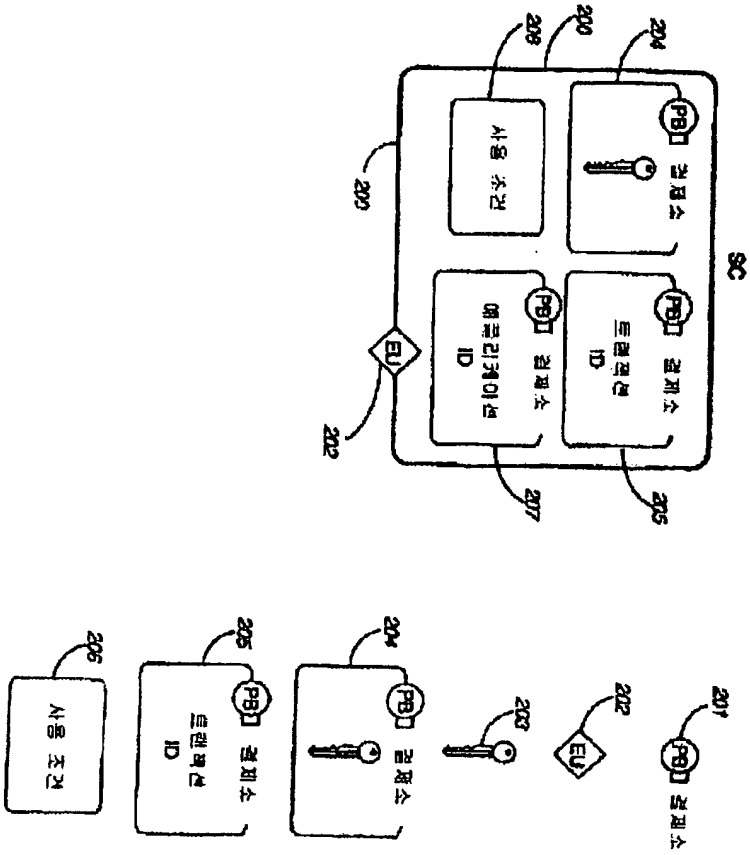
도면 1b


100
105
107
142
143
144
146
148
150
151
182
183
184
186
J
I
H
G
F
E
D
계산서 통합 서브시스템
지불 옵션 인터페이스
고객 서비스 인터페이스
회계 감사 로그
외부의 컴퓨터 통신 부
외부의 컴퓨터 통신 부
PBD 공개 수
PBD 공개 수
PBD 공개 수
PB
QB
호출 SC
라이센스 SC
호출 인프라

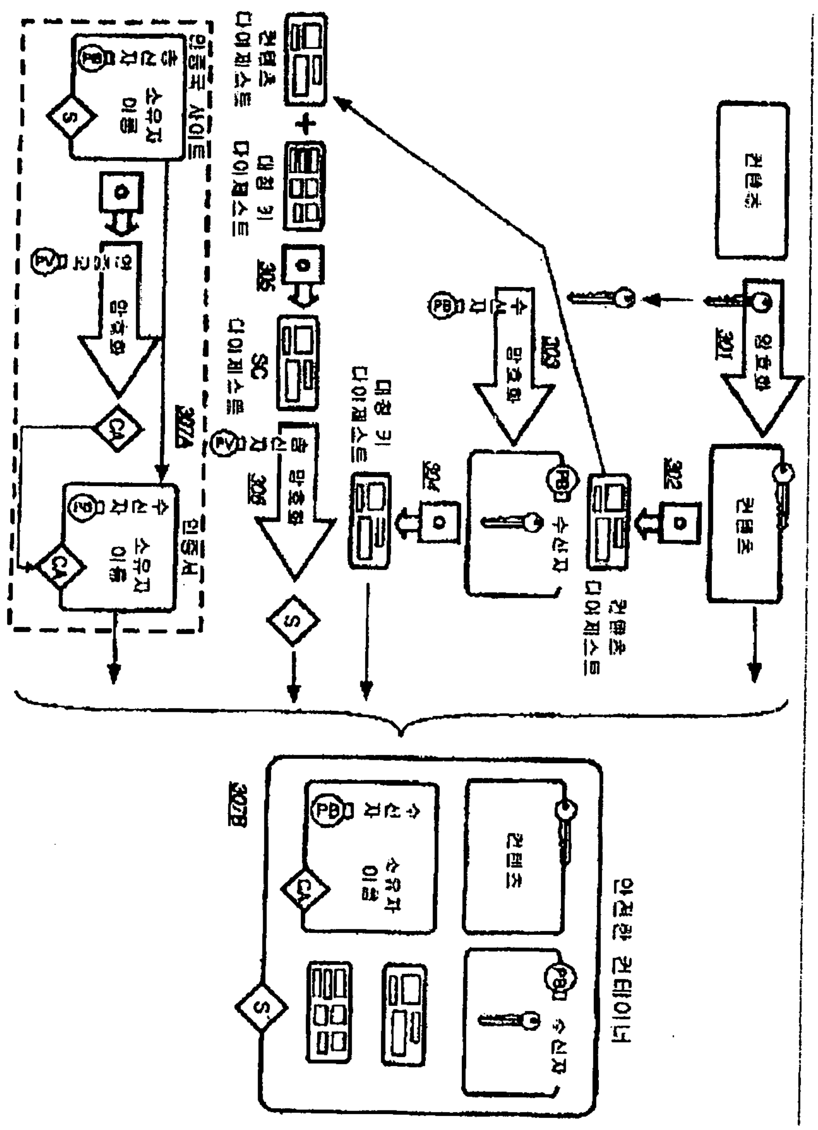
도면5


컨텐츠 호스팅 사이트(들)
컨텐츠 SC
컨텐츠
라이센스 SC
라이센스
HSMS
컨텐츠 라이브러리 관리
엔드 유저 장치(들)
웹 브라우저
인증된 컨텐트 프로세서
웹페이지 렌더링
뷰어 애플릿
암호 툴 키 제공 모듈
라이센스 DB
라이브러리 생성부
렉서
애플리케이션 API
카피/재생 제어
워터마킹 암호화부
디코딩
재생 리스트 생성
라이브러리 관리
재생기

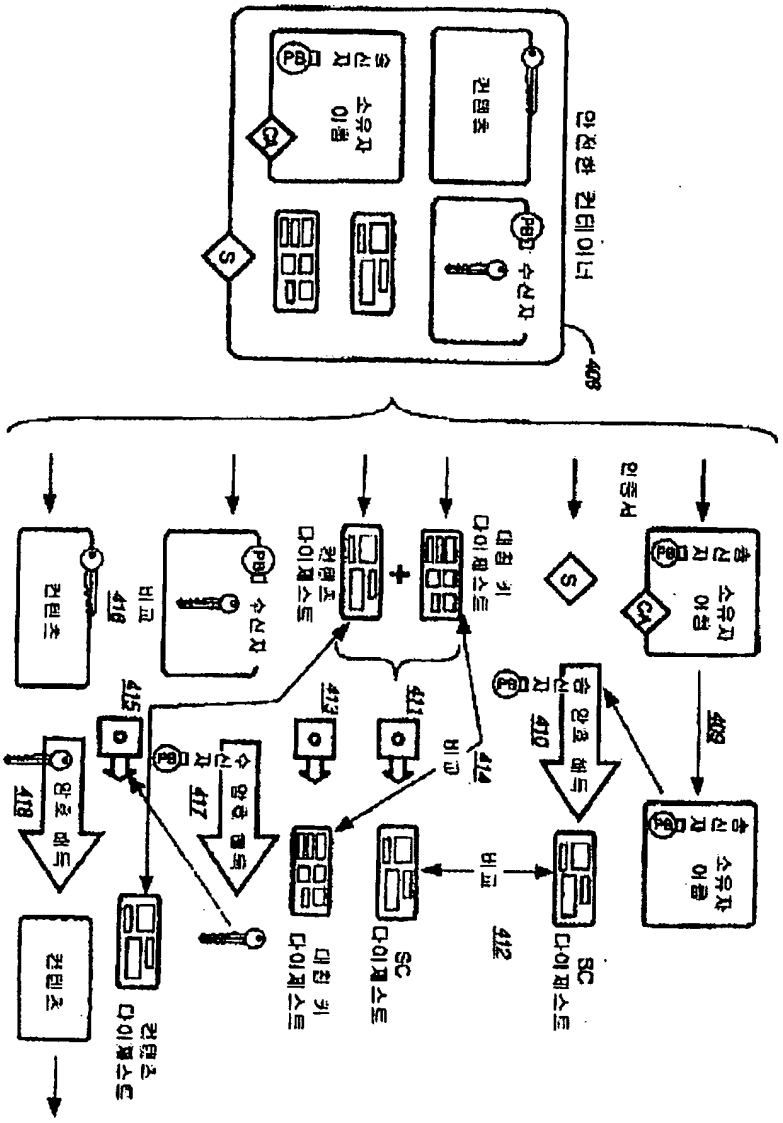
도면2


SC
PB
결제수
트랜잭션 ID
PB
결제수
에스크리케이트 ID
PB
결제수
사용 조건
EU
PB
결제수
PB
결제수
트랜잭션 ID
PB
결제수
사용 조건
201
202
203
204
205
206
207
208
209
200

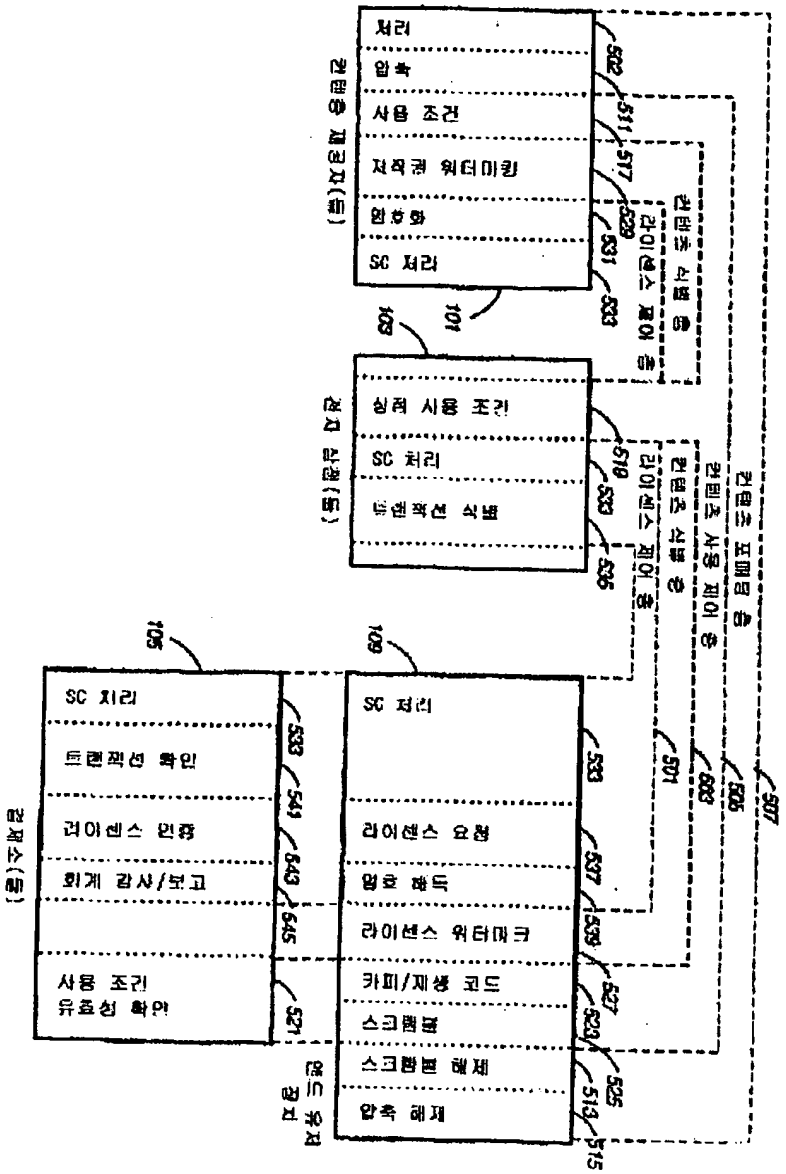
도면3


컨텐츠
암호화
301
컨텐츠
302
컨텐츠 다이제스트
303
수신자
암호화
수신자
304
대칭 키 다이제스트
컨텐츠 다이제스트
대칭 키 다이제스트
305
SC 다이제스트
송신자
암호화
306
S
인증국 사이트
송신자
소유자 이름
S
인증국
암호화
CA
307A
인증서
수신자
소유자 이름
CA
안전한 컨테이너
컨텐츠
수신자
수신자
소유자 이름
CA
S
307B

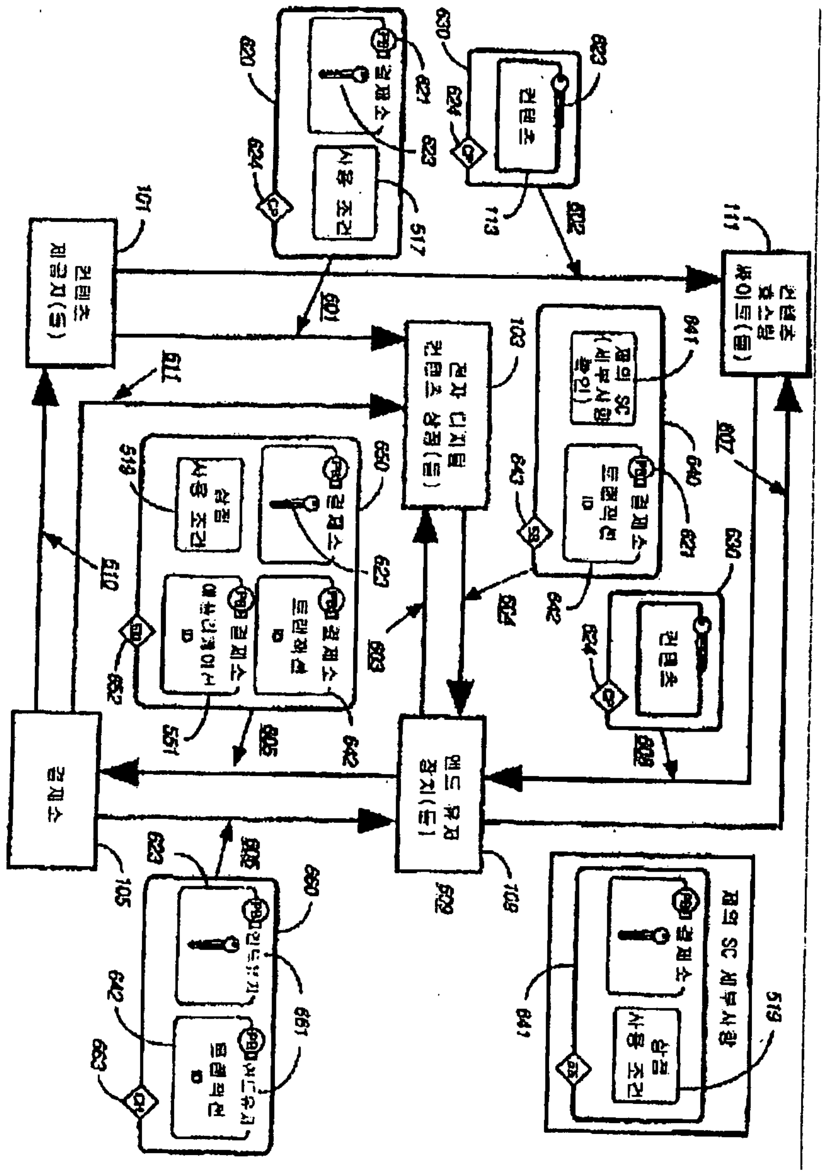
도14


안전한 컨테이너
408
컨테이너
수신자
송신자 이름
S
CA
PB
비교
418
컨테이너
수신자
컨테이너 다이제스트
대칭 키 다이제스트
415
413
411
414
송신자 암호 메뉴
410
409
송신자 이름
암호 메뉴
418
암호 메뉴
417
송신자
대칭 키 다이제스트
SC 다이제스트
비교
412
SC 다이제스트
송신자 이름
컨테이너
컨테이너 다이제스트

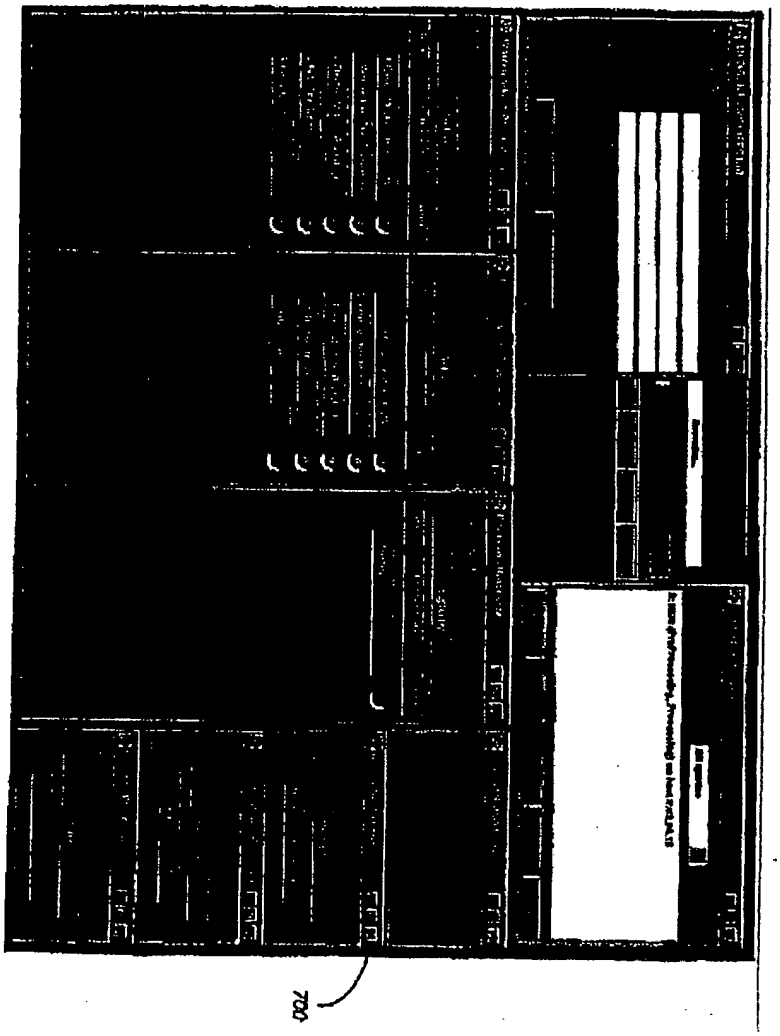
도185


처리
압축
사용 조건
저작권 워터마킹
암호화
SC 처리
콘텐츠 식별 층
라이센스 제어 층
콘텐츠 포매팅 층
콘텐츠 사용 제어 층
라이센스 제어 층
콘텐츠 식별 층
심려 사용 조건
SC 처리
트랜잭션 식별
SC 처리
트랜잭션 확인
라이센스 인증
회계 감사/보고
사용 조건 유효성 확인
SC 처리
라이센스 요청
암호 해독
라이센스 워터마크
카피/재생 코드
스크램블
스크램블 해제
압축 해제
콘텐츠 사용 제어 층
콘텐츠 식별 층
라이센스 제어 층
콘텐츠 포매팅 층
콘텐츠 서버(들)
콘텐츠 식별자(들)
콘텐츠 식별(들)
엔드 유저 장치
101
103
105
107
501
502
503
505
507
511
513
515
517
519
521
523
525
527
529
531
533
535
537
539
541
543
545

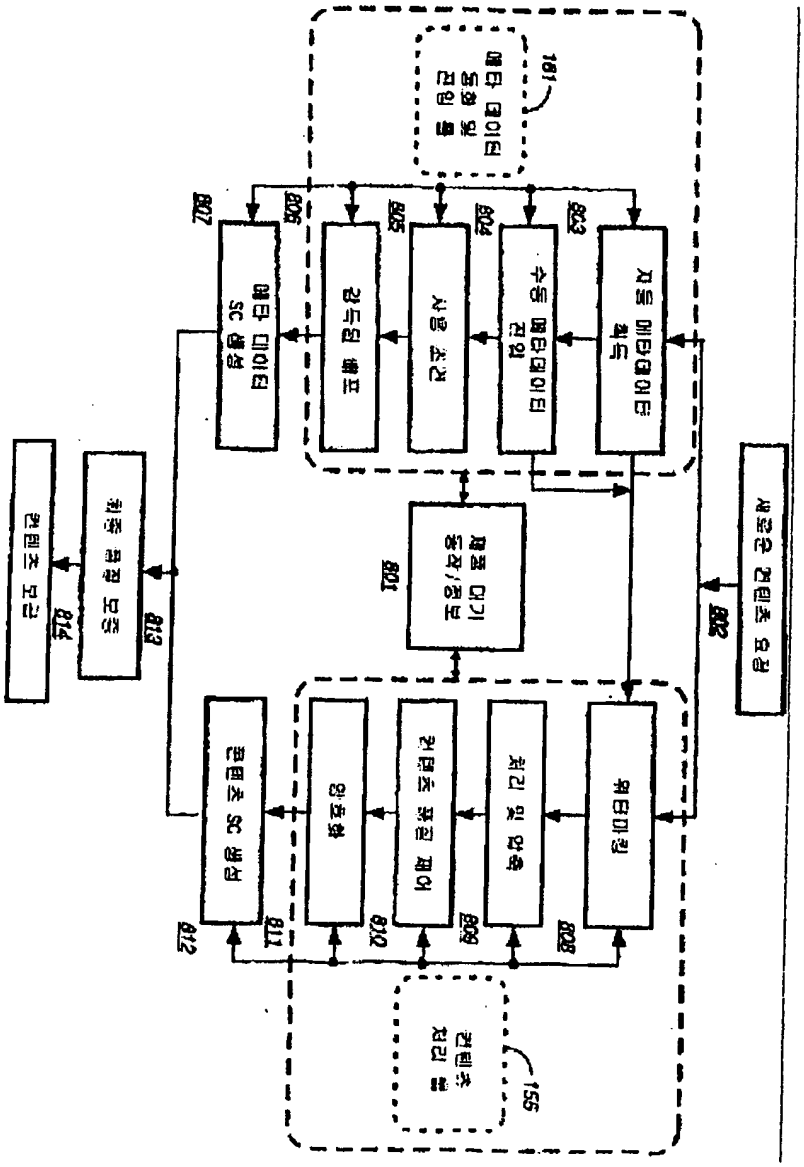
도면8


컨텐츠 제공자(들)
전자 디지털 컨텐츠 상점(들)
컨텐츠 호스팅 사이트(들)
엔드 유저 장치(들)
결제소
컨텐츠
사용 조건
상점 사용 조건
트랜잭션 ID

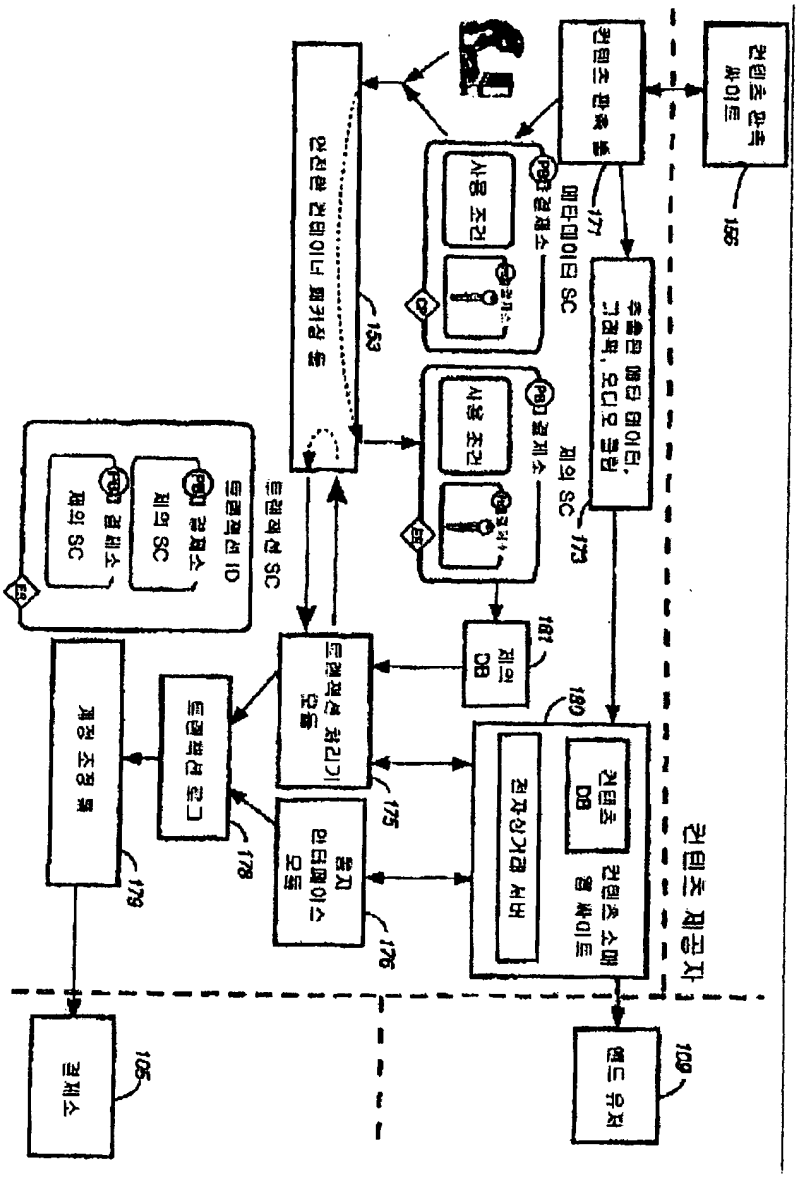
도면7



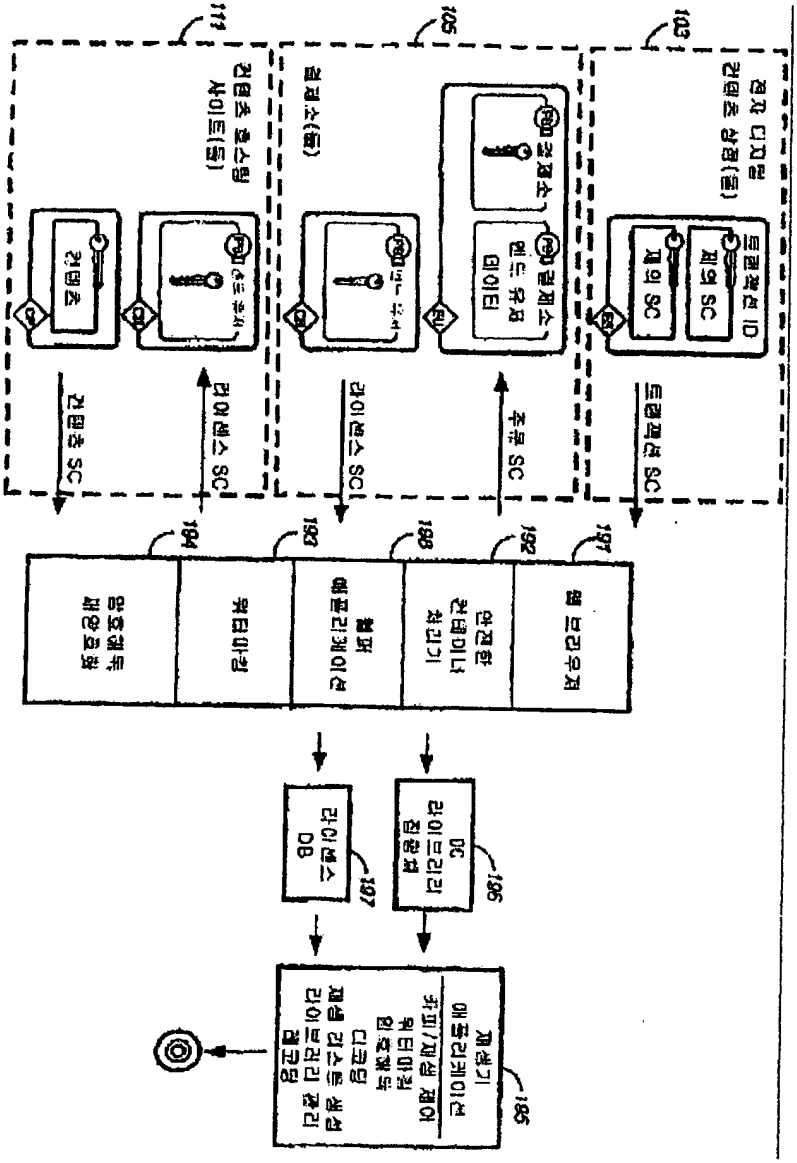
도면4


메타 데이터 관리 블록
161
자동 메타데이터 획득
수동 메타데이터 관리
상황 조건
감독관 배포
메타 데이터 SC 생성
802
803
804
805
806
807
세션 관리 블록
801
워터마킹
처리 및 압축
컨테츠 포맷 파서
암호화
컨테츠 SC 생성부
808
809
810
811
812
155
컨테츠 처리 블록
813
컨테츠 보관
814
세션관 컨테츠 요청

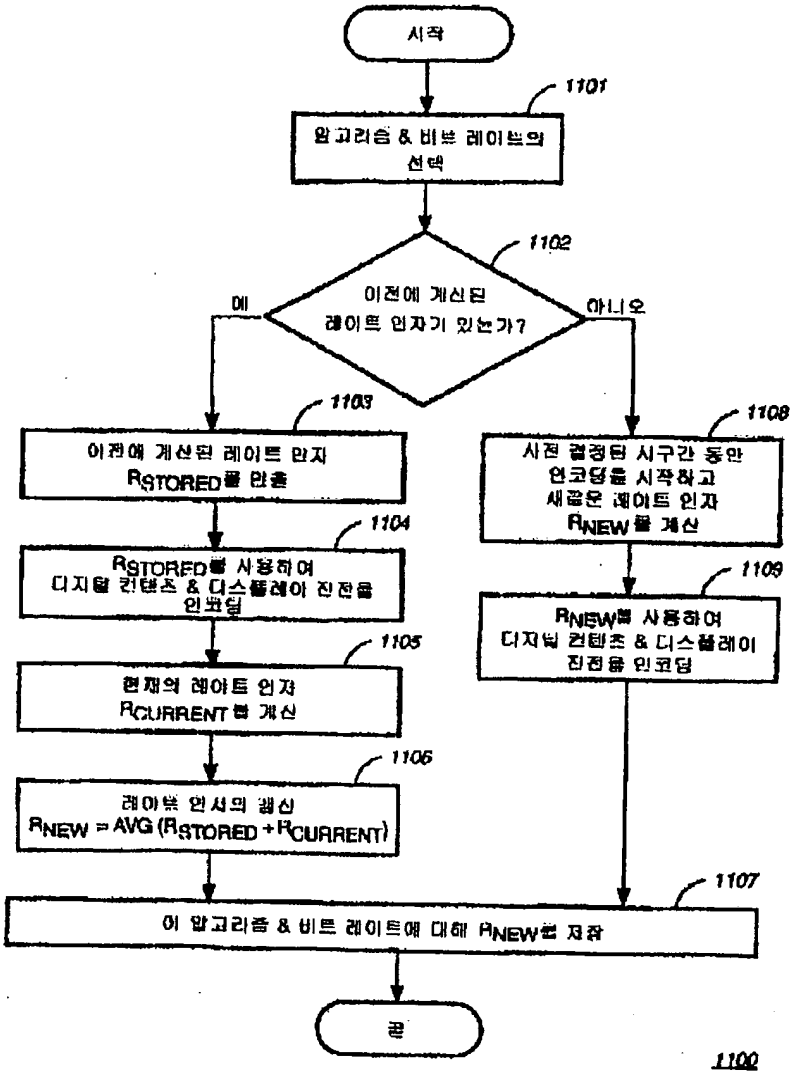
도면


컨텐츠 제공자
컨텐츠 관리 툴
컨텐츠 관리 사이트
155
177
메타데이터 SC
PKID 결제수
사용 조건
추출된 메타 데이터, 그림파일, 오디오 클립
153
안전한 컨테이너 패키징 툴
제의 SC
173
181
제의 DB
189
컨텐츠 DB
전자상거래 서버
컨텐츠 소매 웹 사이트
트랜잭션 처리기 모듈
175
트랜잭션 로그
178
물건 인터페이스 모듈
176
계정 조정 툴
179
트랜잭션 ID
PKID 결제수
제의 SC
PKID 결제수
제의 SC
트랜잭션 SC
결제수
105
엔드 유저
109

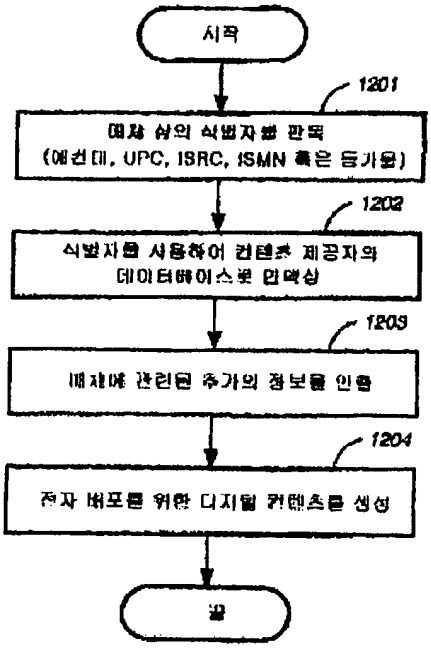
도면10


111
105
103
컨텐츠 프로슈밍 사이트(들)
클리어링(들)
결제수
엔드 유저 데이터
트랜잭션 ID
제어 SC
컨텐츠
컨텐츠 SC
라이센스 SC
주문 SC
트랜잭션 SC
194
193
192
191
보안 및 관리 유저
보안 및 컨텐츠 처리기
패키지
컨텐츠
암호화 및 해독 모듈
197
라이센스 DB
196
DC 라이브러리 집중부
195
제품기 에뮬레이션 유저/제품 제어
뉴티어링 및 보안 모듈
제품 라이브러리 관리
컨텐츠 라이브러리 관리

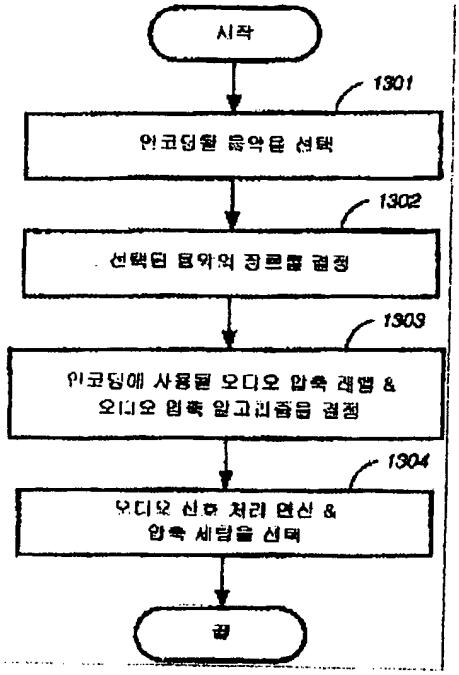
도면11


시작
1101
알고리즘 & 비트 레이트의 선택
1102
이전에 계산된 레이트 인자가 있는가?
예
아니오
1103
이전에 계산된 레이트 인자 R_{STORED}를 얻음
1104
R_{STORED}를 사용하여 디지털 컨텐츠 & 디스플레이 전전을 인코딩
1105
현재의 레이트 인자 $R_{CURRENT}$를 계산
1106
레이트 인자의 갱신 $R_{NEW} = AVG(R_{STORED} + R_{CURRENT})$
1108
사전 결정된 시구간 동안 인코딩을 시작하고 새로운 레이트 인자 R_{NEW}를 계산
1109
R_{NEW}를 사용하여 디지털 컨텐츠 & 디스플레이 전전을 인코딩
1107
이 알고리즘 & 비트 레이트에 대해 R_{NEW}를 저장
끝
1100

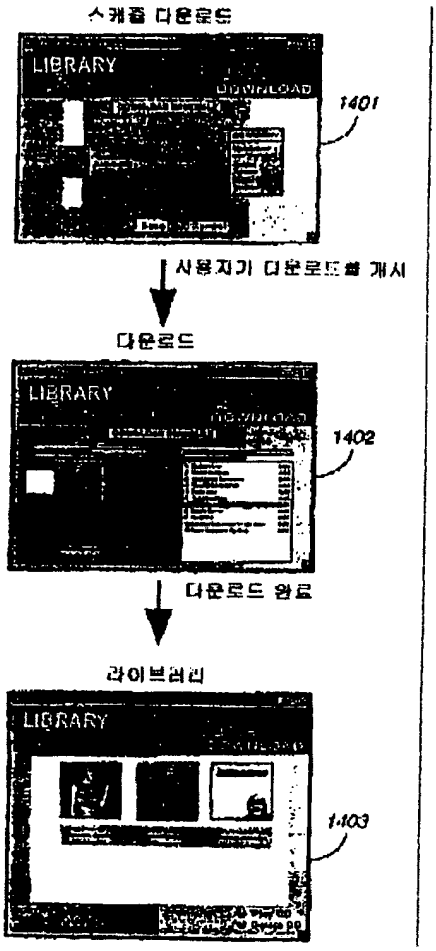
도면12


시작
1201
매체 상의 식별자를 판독
(예컨대, UPC, ISRC, ISMN 혹은 등가물)
1202
식별자를 사용하여 컨텐츠 제공자의
데이터베이스로 인덱싱
1203
매체에 관련된 추가의 정보를 인출
1204
전자 배포를 위한 디지털 컨텐츠를 생성
끝

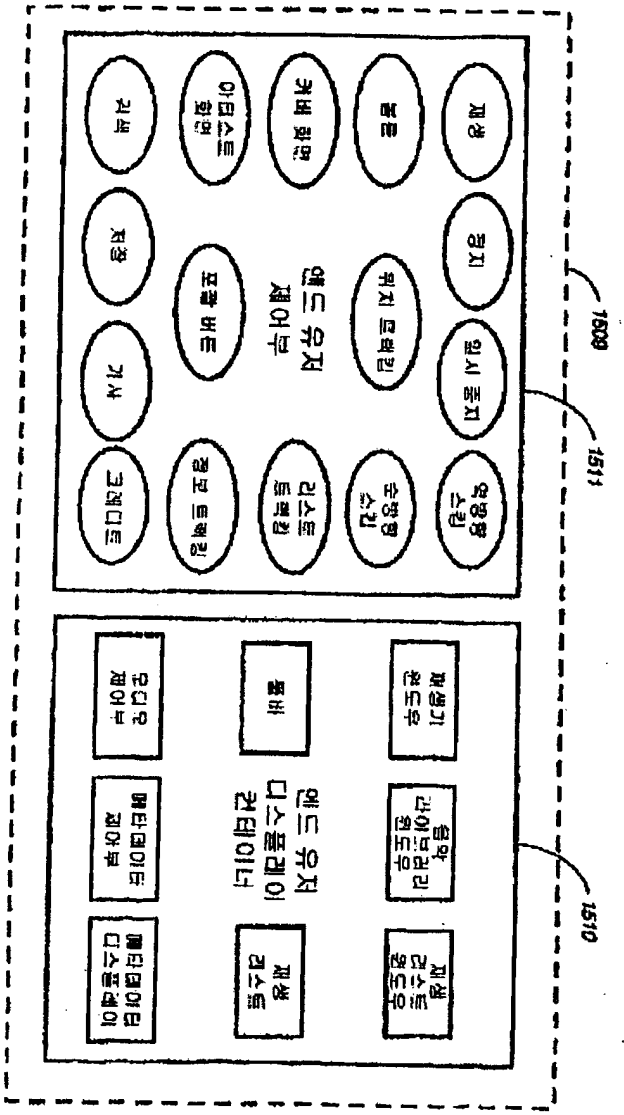
도면13


시작
1301
인코딩될 음악을 선택
1302
선택된 음악의 장르를 결정
1303
인코딩에 사용될 오디오 압축 레벨 &
오디오 압축 알고리즘을 결정
1304
오디오 신호 처리 변신 &
압축 세팅을 선택
끝

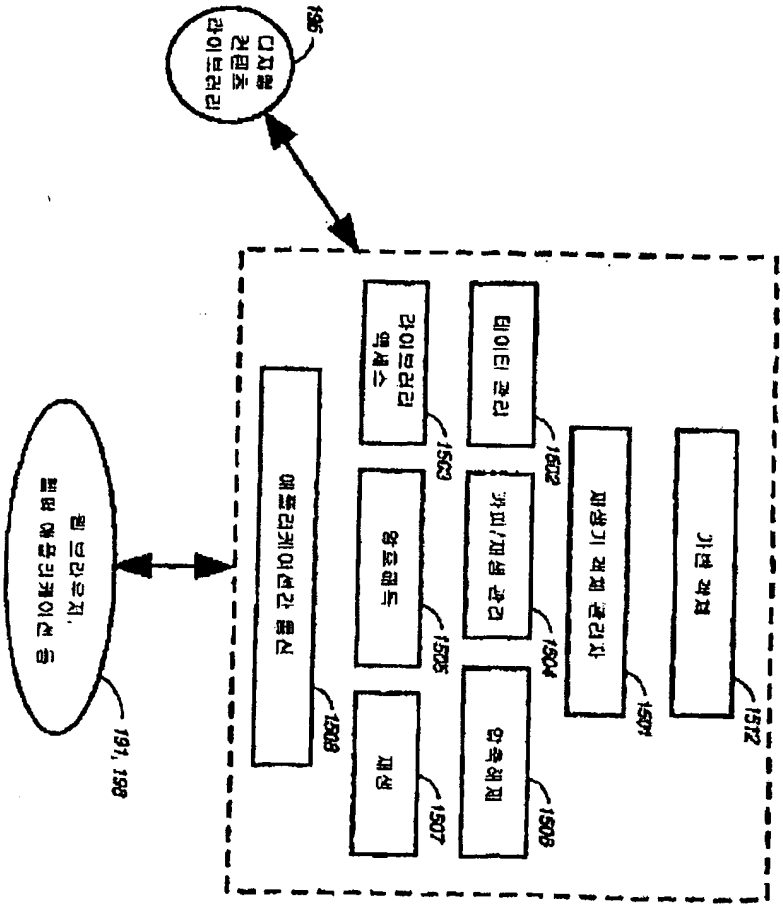
도면14


스케줄 다운로드
LIBRARY
1401
사용자가 다운로드를 개시
다운로드
LIBRARY
1402
다운로드 완료
라이브러리
LIBRARY
1403

도면15


1509
1511
1510
재생
정지
일시 정지
탐색
위치 표시줄
캐쉬 화면
아티스트 화면
검색
저장
기사
그래디트
엔드 유저 제어부
포털 버튼
결과 트랙킹
리스트 트랙킹
순방향 스킵
역방향 스킵
재생기 관리자
음악 라이브러리 관리자
재생 리스트 관리자
툴바
재생 리스트
엔드 유저 디스플레이 관리 에이전트
윈도우 제어부
메타데이터 제어부
메타데이터 디스플레이

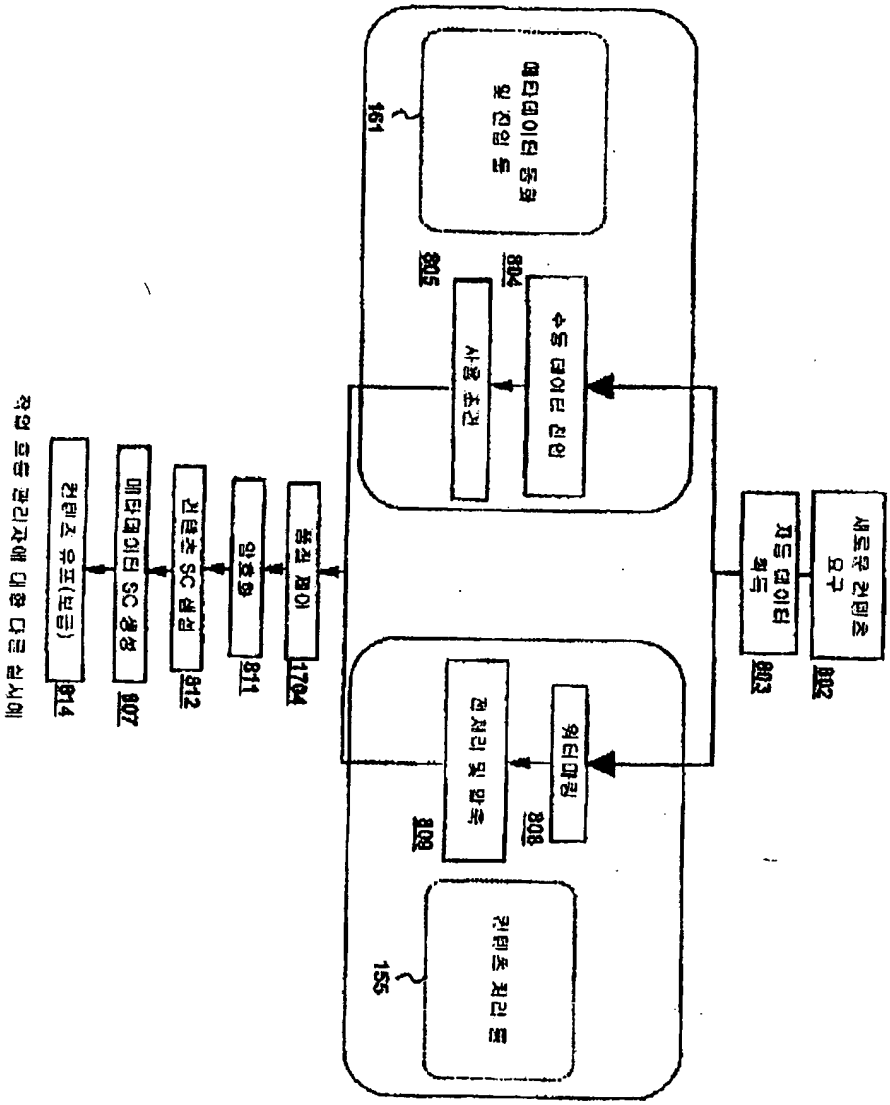
도면15b


186
디지털 컨텐츠 라이브러리
191, 198
멀티미디어 응용 프로그램 인터페이스
1502
데이터 로더
1503
라이브러리 빌더
1504
파일/자원 관리
1505
암호화 도구
1506
애플리케이션간 통신
1507
제어
1508
안전 체제
1509
파일 시스템 관리자
1512
기타 객체

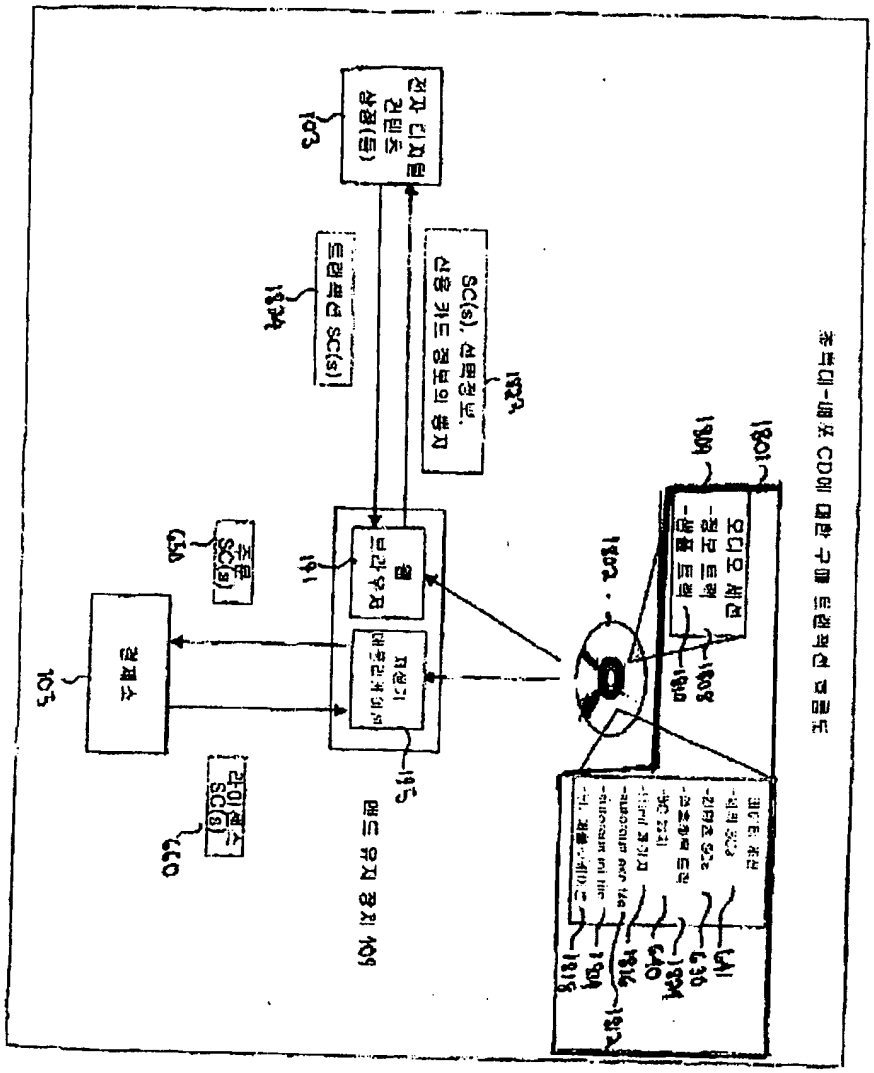
도면17

1604
1602
재생기
클립 캐쉬 서버
클립
1605
인쇄
이미지 디스플레이
사용자가 재생 리스트를 선택
1601
클라이언트
사용자가 재생 리스트를 선택
1603
재생 리스트

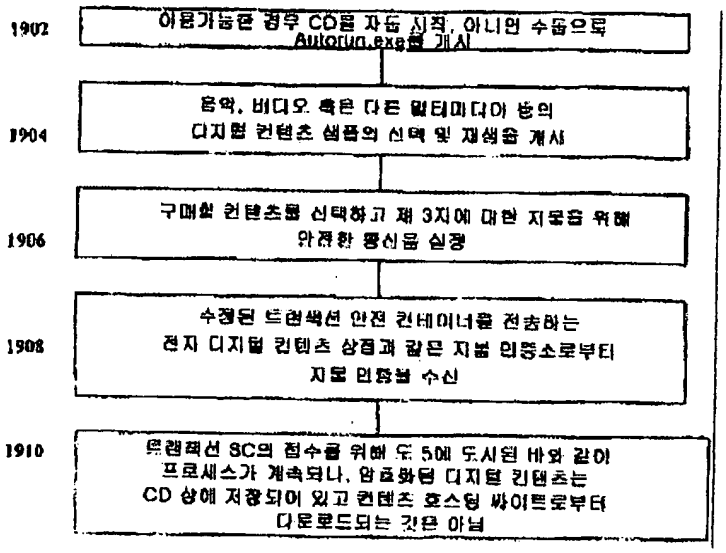
도면17


151
메타데이터 동화 및 관리 툴
804
수동 데이터 입력
805
사용자 인터
802
서드파티 응용
803
서드파티 데이터 획득
808
워터마킹
809
권리관리 및 암호화
155
컨텐츠 처리 툴
1704
동기 데이
811
암호화
812
보호된 SC 생성
807
메타데이터 SC 생성
814
컨테이너 포맷(들)
컨텐츠 및 메타데이터 다른 컴퓨터에

도면8


초고대-배포 CD에 대한 수퍼 트레일러 프로토
오디오 재생
-정보 트랙
-음악 트랙
전자 디지털 상점(들)
트랙북마크 SC(s)
SC(s), 선물증명서, 신용 카드 정보의 송신
플
브라우저
지원기
초콜릿 SC(s)
결제수
전자 SC(s)
메모리 유지 장치 405

도면 19


1902
이용가능한 경우 CD를 자동 시작, 아니면 수동으로 Autorun.exe를 개시
1904
음악, 비디오 혹은 다른 멀티미디어 등의 디지털 컨텐츠 샘플의 선택 및 재생을 개시
1906
구매할 컨텐츠를 선택하고 제 3자에 대한 지불을 위해 안전한 통신을 실행
1908
수정된 트랜잭션 안전 컨테이너를 전송하는 전자 디지털 컨텐츠 상점과 같은 지불 인증소로부터 지불 인증을 수신
1910
트랜잭션 SC의 점수를 위해 도 5에 도시된 바와 같이 프로세스가 계속되나, 암호화된 디지털 컨텐츠는 CD 상에 저장되어 있고 컨텐츠 호스팅 사이트로부터 다운로드되는 것은 아님